ZyWALL USG 1000

Unified Security Gateway

User's Guide

Version 2.00
10/2007
Edition 1

DEFAULT LOGIN	
LAN Port	**P1**
IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

This manual is designed to guide you through the configuration of your ZyWALL for its various applications. Generally, it is organized as follows.

- Introduction (ZyWALL, web configurator)
- Features (by menu item in the web configurator)
    - Overview, including background
    - Web Configurator screens
- Appendices

Intended Audience

This manual is intended for network administrators, or people who have a good knowledge of TCP/IP networking concepts and topology, who want to want to configure the ZyWALL using the web configurator.

1. Read Chapter 1 on page 53 chapter for an overview of features available on the ZyWALL.
2. Read Chapter 3 on page 65 for web browser requirements and an introduction to the main components, icons and menus in the ZyWALL web configurator.
3. Read Chapter 4 on page 75 if you're using the wizards for first time setup and you want more detailed information than what the real time online help provides.
4. It is highly recommended you read Chapter 5 on page 111 for detailed information on essential terms used in the ZyWALL, what prerequisites are needed to configure a feature and how to use that feature.
5. It is highly recommended you read Chapter 6 on page 125 for multiple ZyWALL application examples.
6. Subsequent chapters are arranged by menu item as defined in the web configurator. Read each chapter carefully for detailed information on that menu item.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to show you how to make the ZyWALL hardware connections, rack mounting and access the web configurator wizards. (See the wizard real time help for information on configuring each screen.) It contains a connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- Configuration Reference Card
  See this handy reference card to see what prerequisites are needed to configure a feature and how to use this feature in the ZyWALL.
- CLI Reference Guide
  The CLI Reference Guide explains how to use the Command-Line Interface (CLI) to configure the ZyWALL.

It is recommended you use the web configurator to configure the ZyWALL.

- Web Configurator Online Help
  Click the help icon in any screen for help in configuring that screen and supplementary information.
- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

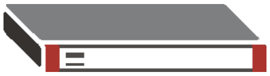
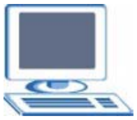
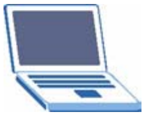
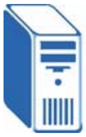
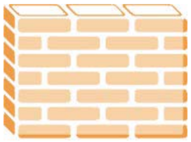
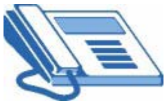
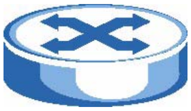
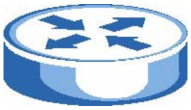
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ZyWALL USG1000 may be referred to as the "ZyWALL", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance** > **Log** > **Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyWALL icon is not an exact representation of your device.

ZyWALL 	Computer 	Notebook computer 
Server 	Firewall 	Telephone 
Switch 	Router 	

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

This product is recyclable. Dispose of it properly.

Contents Overview

Introduction 51

Introducing the ZyWALL 53
Features and Applications 57
Web Configurator 65
Wizard Setup 75
Configuration Basics 111
Tutorials 125
Status 157
Registration 165
Update 171

Network 177

Interface 179
Trunks 219
Policy and Static Routes 225
Routing Protocols 235
Zones 245
DDNS 249
Virtual Servers 255
HTTP Redirect 261
ALG 265

Firewall and VPN 275

Firewall 277
IPSec VPN 291
SSL VPN 323
SSL User Screens 331
SSL User Application Screens 337
SSL User File Sharing Screens 339
L2TP VPN 345
L2TP VPN Example 351

Application Patrol & Anti-X 377

Application Patrol 379
Anti-Virus 403
IDP 417
ADP 445

Content Filter Screens 463
Content Filter Reports 483

Device HA & Objects 491

Device HA 493
User/Group 503
Addresses 515
Services 521
Schedules 527
AAA Server 531
Authentication Objects 541
Certificates 545
ISP Accounts 563
SSL Application 567

System 573

System 575
Service Control 587

Maintenance & Troubleshooting 613

File Manager 615
Logs 625
Reports 637
Diagnostics 647
Reboot 649
Troubleshooting 651

Appendices and Index 655

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

List of Figures 31

List of Tables 43

Part I: Introduction 51

Chapter 1
Introducing the ZyWALL 53

1.1 Overview and Key Default Settings 53
1.2 Front Panel LEDs 53
1.3 Management Overview 54
1.4 Starting and Stopping the ZyWALL 55

Chapter 2
Features and Applications 57

2.1 Features 57
2.2 Packet Flow 58
  2.2.1 Interface to Interface (Through ZyWALL) 59
  2.2.2 Interface to Interface (To/From ZyWALL) 59
  2.2.3 Interface to Interface (From VPN Tunnel) 59
  2.2.4 Interface to Interface (To VPN Tunnel) 59
2.3 Applications 60
  2.3.1 VPN Connectivity 60
  2.3.2 SSL VPN Network Access 60
  2.3.3 User-Aware Access Control 61
  2.3.4 Multiple WAN Interfaces 62
  2.3.5 Device HA 62

Chapter 3
Web Configurator 65

3.1 Web Configurator Requirements 65
3.2 Web Configurator Access 65
3.3 Web Configurator Main Screen 67
    3.3.1 Title Bar 67
    3.3.2 Navigation Panel 68
    3.3.3 Main Window 71
    3.3.4 Message Bar 72

Chapter 4
Wizard Setup 75

4.1 Wizard Setup Overview 75
4.2 Installation Setup, One ISP 76
4.3 Step 1 Internet Access 77
    4.3.1 Ethernet: Auto IP Address Assignment 78
    4.3.2 Ethernet: Static IP Address Assignment 78
    4.3.3 Step 2 Internet Access Ethernet 80
    4.3.4 PPPoE: Auto IP Address Assignment 81
    4.3.5 PPPoE: Static IP Address Assignment 82
    4.3.6 Step 2 Internet Access PPPoE 84
    4.3.7 PPTP: Auto IP Address Assignment 85
    4.3.8 PPTP: Static IP Address Assignment 88
    4.3.9 Step 2 Internet Access PPTP 89
    4.3.10 Step 4 Internet Access - Finish 91
4.4 Device Registration 91
4.5 Installation Setup, Two Internet Service Providers 93
    4.5.1 Internet Access Wizard Setup Complete 95
4.6 VPN Setup 95
4.7 VPN Wizards 96
    4.7.1 VPN Express Wizard 97
4.8 VPN Express Wizard - Remote Gateway 97
    4.8.1 VPN Express Wizard - Policy Setting 99
    4.8.2 VPN Express Wizard - Summary 100
    4.8.3 VPN Express Wizard - Finish 101
    4.8.4 VPN Advanced Wizard 101
    4.8.5 VPN Advanced Wizard - Remote Gateway 103
    4.8.6 VPN Advanced Wizard - Phase 1 105
    4.8.7 VPN Advanced Wizard - Phase 2 107
    4.8.8 VPN Advanced Wizard - Summary 108
    4.8.9 VPN Advanced Wizard - Finish 109

Chapter 5
Configuration Basics 111

5.1 Granular Configuration 111

5.2 Terminology in the ZyWALL 112
5.3 Physical Ports, Interfaces, and Zones 112
    5.3.1 Network Topology Example 113
5.4 Feature Configuration Overview 114
    5.4.1 Feature 114
    5.4.2 Interface 115
    5.4.3 Trunks 115
    5.4.4 IPSec VPN 116
    5.4.5 SSL VPN 116
    5.4.6 L2TP VPN 116
    5.4.7 Zones 116
    5.4.8 Device HA 117
    5.4.9 DDNS 117
    5.4.10 Policy Routes 117
    5.4.11 Static Routes 118
    5.4.12 Firewall 118
    5.4.13 Application Patrol 119
    5.4.14 Anti-Virus 120
    5.4.15 IDP 120
    5.4.16 ADP 120
    5.4.17 Content Filter 120
    5.4.18 Virtual Server (Port Forwarding) 121
    5.4.19 HTTP Redirect 121
    5.4.20 ALG 122
5.5 Objects 122
    5.5.1 User/Group 122
5.6 System Management and Maintenance 123
    5.6.1 DNS, WWW, SSH, TELNET, FTP, SNMP, Dial-in Mgmt, Vantage CNM 123
    5.6.2 File Manager 124
    5.6.3 Licensing Registration 124
    5.6.4 Licensing Update 124
    5.6.5 Logs and Reports 124
    5.6.6 Diagnostics 124

Chapter 6
Tutorials 125

6.1 Interfaces and Zones 125
    6.1.1 Set up Port Grouping 125
    6.1.2 Set up Ethernet Interfaces 127
    6.1.3 WAN Trunk 129
    6.1.4 Zones 130
6.2 IPSec VPN 132
    6.2.1 Set up the Ethernet Interfaces and Zones 132

6.2.2 Set up the VPN Gateway 132
6.2.3 Set up the VPN Connection 133
6.2.4 Set up the Policy Route for the VPN Tunnel 134
6.2.5 Set up the Zone for the VPN Tunnel 135
6.3 Device HA 136
6.3.1 Set up DNS for the Virtual Router 136
6.3.2 Set up the VRRP Groups on the Master 136
6.3.3 Set up the Password for Synchronization 138
6.3.4 Finish Configuring the Master 139
6.3.5 Set up the Ethernet Interfaces on the Backup 139
6.3.6 Set up the VRRP Groups on the Backup 139
6.3.7 Synchronize the Backup 140
6.4 User-Aware Access Control 140
6.4.1 Set up User Accounts 141
6.4.2 Set up User Groups 141
6.4.3 Set up User Authentication Using the RADIUS Server 142
6.4.4 Set up Web Surfing Policies With Bandwidth Restrictions 143
6.4.5 Set up MSN Policies 144
6.4.6 Set up LAN-to-DMZ Policies 145
6.5 Trunks 146
6.5.1 Set up Available Bandwidth on Ethernet Interfaces 146
6.5.2 Change WAN Trunk Algorithm 147
6.6 NAT 1:1 Example 147
6.6.1 NAT 1:1 Address Objects 148
6.6.2 NAT 1:1 Virtual Server 149
6.6.3 NAT 1:1 Policy Route 149
6.6.4 NAT 1:1 Firewall Rule 150
6.7 NAT Loopback 151
6.7.1 NAT Loopback Virtual Server 152
6.7.2 NAT Loopback Policy Route 153
6.8 Service Control and the Firewall 155
6.8.1 Allowing HTTPS Administrator Access Only From the LAN 155

Chapter 7
Status 157

7.1 Status Screen 157
7.2 VPN Status 160
7.3 DHCP Table 161
7.4 Port Statistics 162
7.5 Current Users 163

Chapter 8
Registration 165

8.1 myZyXEL.com Overview 165
    8.1.1 Subscription Services Available on the ZyWALL 165
8.2 Registration 166
8.3 Service 168

Chapter 9
Update 171

9.1 Updating Anti-virus Signatures 171
9.2 Updating IDP and Application Patrol Signatures 173
9.3 Updating System Protect Signatures 175

Part II: Network 177

Chapter 10
Interface 179

10.1 Interface Overview 179
    10.1.1 Types of Interfaces 179
    10.1.2 IP Address Assignment 180
    10.1.3 Interface Parameters 182
    10.1.4 DHCP Settings 182
    10.1.5 Ping Check Settings 183
    10.1.6 Relationships Between Interfaces 184
10.2 Ethernet Interfaces 184
    10.2.1 Ethernet Interfaces Overview 184
    10.2.2 Interface Summary Screen 185
    10.2.3 Ethernet Summary Screen 188
    10.2.4 Ethernet Edit 189
10.3 Port Grouping 194
    10.3.1 Port Grouping Overview 194
    10.3.2 Port Grouping Screen 195
10.4 VLAN Interfaces 196
    10.4.1 VLAN Overview 196
    10.4.2 VLAN Interfaces Overview 198
    10.4.3 VLAN Summary Screen 198
    10.4.4 VLAN Add/Edit 199
10.5 Bridge Interfaces 203
    10.5.1 Bridge Overview 204
    10.5.2 Bridge Interface Overview 205
    10.5.3 Bridge Summary 205
    10.5.4 Bridge Add/Edit 206
10.6 PPPoE/PPTP Interfaces 210

10.6.1 PPPoE/PPTP Overview 210
10.6.2 PPPoE/PPTP Interfaces Overview 211
10.6.3 PPPoE/PPTP Interface Summary 212
10.6.4 PPPoE/PPTP Interface Add/Edit 213
10.7 Auxiliary Interface 215
10.7.1 Auxiliary Interface Overview 215
10.7.2 Auxiliary 215
10.8 Virtual Interfaces 217
10.8.1 Virtual Interfaces Add/Edit 217

Chapter 11
Trunks 219

11.1 Trunks Overview 219
11.2 Trunk Scenario Examples 219
11.3 Load Balancing Introduction 219
11.4 Load Balancing Algorithms 220
11.4.1 Least Load First 220
11.4.2 Weighted Round Robin 221
11.4.3 Spillover 221
11.5 Trunk Summary 222
11.6 Configuring a Trunk 222

Chapter 12
Policy and Static Routes 225

12.1 Policy Route 225
12.1.1 Benefits 225
12.2 Routing Policy 225
12.2.1 NAT and SNAT 226
12.2.2 Port Triggering 226
12.2.3 Maximize Bandwidth Usage 227
12.2.4 Reserving Bandwidth for Non-Bandwidth Class Traffic 227
12.3 IP Routing Policy Setup 227
12.4 Policy Route Edit 229
12.5 IP Static Routes 232
12.6 Static Route Summary 233
12.7 Edit a Static Route 233

Chapter 13
Routing Protocols 235

13.1 Routing Protocols Overview 235
13.1.1 RIP Overview 235
13.1.2 Authentication Types 236
13.2 RIP Screen 236

13.3 OSPF Overview 237
13.3.1 OSPF Areas 238
13.3.2 OSPF Routers 239
13.3.3 Virtual Links 240
13.3.4 OSPF Configuration 240
13.4 OSPF Screens 241
13.4.1 OSPF Summary 241
13.4.2 OSPF Area Add/Edit 242

Chapter 14
Zones 245

14.1 Zones Overview 245
14.1.1 Effect of Zones on Different Types of Traffic 245
14.2 Zone Summary 246
14.3 Zone Add/Edit 247

Chapter 15
DDNS 249

15.1 DDNS Overview 249
15.1.1 DYNDNS Wildcard 249
15.1.2 High Availability (HA) 250
15.1.3 Mail Exchanger 250
15.2 DDNS Screens 250
15.3 DDNS Summary 251
15.4 Dynamic DNS Add/Edit 252

Chapter 16
Virtual Servers 255

16.1 Virtual Server Overview 255
16.2 Virtual Server Example 256
16.3 Virtual Server Screens 256
16.4 Virtual Server Summary Screen 256
16.4.1 Virtual Server Add/Edit 258

Chapter 17
HTTP Redirect 261

17.1 HTTP Redirect Overview 261
17.1.1 Web Proxy Server 261
17.2 HTTP Redirect, Firewall and Policy Route 261
17.3 Configuring HTTP Redirect 262
17.4 HTTP Redirect Edit 263

Chapter 18
ALG 265

18.1 ALG Introduction 265
    18.1.1 Application Layer Gateway (ALG) and NAT 265
    18.1.2 ALG and Trunks 265
    18.1.3 FTP 266
    18.1.4 H.323 266
    18.1.5 RTP 266
    18.1.6 SIP 267
18.2 Peer-to-Peer Calls and the ZyWALL 268
    18.2.1 VoIP Calls from the WAN with Multiple Outgoing Calls 268
    18.2.2 VoIP with Multiple WAN IP Addresses 268
18.3 ALG Screen 269
18.4 WAN to LAN SIP Peer-to-peer Calls Example 271

Part III: Firewall and VPN........ 275

Chapter 19
Firewall........ 277

19.1 Firewall Overview 277
19.2 Firewall Rules 278
    19.2.1 Rule Directions 278
    19.2.2 Firewall and VPN Traffic 280
19.3 Firewall Rule Example Applications 280
19.4 Alerts 282
19.5 Asymmetrical Routes 282
    19.5.1 Virtual Interfaces and Asymmetrical Routes 283
19.6 Configuring the Firewall 283
    19.6.1 Edit a Firewall Rule 286
19.7 Firewall Rule Configuration Example 287

Chapter 20
IPSec VPN........ 291

20.1 IPSec VPN Overview 291
    20.1.1 IPSec SA Overview 292
    20.1.2 Additional Topics for IPSec SA 294
20.2 VPN Related Configuration 296
20.3 VPN Connection Screens 297
    20.3.1 VPN Connection Summary 297
    20.3.2 VPN Connection Add/Edit IKE 298
    20.3.3 VPN Connection Add/Edit Manual Key 302
20.4 VPN Gateway Screens 306
    20.4.1 IKE SA Overview 306

20.4.2 Additional Topics for IKE SA 310
20.4.3 VPN Gateway Summary 312
20.4.4 VPN Gateway Add/Edit 313
20.5 VPN Concentrator 318
20.5.1 VPN Concentrator Summary 319
20.5.2 VPN Concentrator Add/Edit 319
20.6 SA Monitor Screen 320
20.6.1 Regular Expressions in Searching IPSec SAs by Name or Policy 322

Chapter 21
SSL VPN........ 323

21.1 SSL Access Policy 323
21.1.1 SSL Access Policy Objects 323
21.1.2 SSL Access Policy Limitations 324
21.2 SSL Access Privilege List 324
21.3 Creating/Editing an SSL Access Policy 325
21.4 SSL Connection Monitor 326
21.5 Configuring SSL Global Setting 327
21.5.1 Uploading a Custom Logo 329
21.6 Establishing an SSL VPN Connection 329

Chapter 22
SSL User Screens 331

22.1 Overview 331
22.1.1 Network Resource Access Methods 331
22.1.2 System Requirements 331
22.1.3 Information You Need 332
22.1.4 Certificates 332
22.2 Remote User Login 332
22.3 SSL VPN User Screens 334
22.4 Bookmark 335
22.5 Logout 335

Chapter 23
SSL User Application Screens 337

23.1 Overview 337
23.1.1 The Application Screen 337

Chapter 24
SSL User File Sharing Screens 339

24.1 Overview 339
24.2 Main File Sharing Screen 339
24.3 Opening a File or Folder 340

24.3.1 Downloading a File 341
24.3.2 Saving a File 341
24.4 Creating a New Folder 342
24.5 Renaming a File or Folder 342
24.6 Deleting a File or Folder 343
24.7 Uploading a File 344

Chapter 25
L2TP VPN.. 345

25.1 L2TP VPN Overview 345
25.2 IPSec Configuration 345
25.2.1 Using the Default L2TP VPN Connection 346
25.3 Policy Route 346
25.4 L2TP VPN Configuration 347
25.5 L2TP VPN Session Monitor 348

Chapter 26
L2TP VPN Example.. 351

26.1 L2TP VPN Example 351
26.2 Configuring the Default L2TP VPN Gateway Example 351
26.3 Configuring the Default L2TP VPN Connection Example 353
26.4 Configuring the L2TP VPN Settings Example 354
26.5 Configuring the Policy Route for L2TP Example 354
26.6 Configuring L2TP VPN in Windows XP and 2000 355
26.6.1 Configuring L2TP in Windows XP 356
26.6.2 Configuring L2TP in Windows 2000 361

Part IV: Application Patrol & Anti-X.. 377

Chapter 27
Application Patrol.. 379

27.1 Application Patrol Overview 379
27.2 Classification of Applications 379
27.3 Configurable Application Policies 380
27.4 Bandwidth Management 380
27.4.1 Connection and Packet Directions 381
27.4.2 Outbound and Inbound Bandwidth Limits 381
27.4.3 Bandwidth Management Priority 382
27.4.4 Maximize Bandwidth Usage 382
27.4.5 Bandwidth Management Behavior 382
27.5 Application Patrol Bandwidth Management Examples 384

27.5.1 Setting the Interface’s Bandwidth 385
27.5.2 SIP Any to WAN Bandwidth Management Example 385
27.5.3 SIP WAN to Any Bandwidth Management Example 386
27.5.4 HTTP Any to WAN Bandwidth Management Example 386
27.5.5 FTP WAN to DMZ Bandwidth Management Example 386
27.5.6 FTP LAN to DMZ Bandwidth Management Example 387
27.6 Other Applications 388
27.7 Application Patrol Screens 388
27.8 Application Patrol General 388
27.9 Application Patrol Applications 390
27.9.1 Application Patrol Edit 391
27.9.2 Application Patrol Policy Edit 393
27.10 Other Protocol Screen 395
27.10.1 Other Configuration Add/Edit 397
27.11 Application Patrol Statistics 399
27.11.1 Application Patrol Statistics: General Setup 399
27.11.2 Application Patrol Statistics: Bandwidth Statistics 400
27.11.3 Application Patrol Statistics: Protocol Statistics 400

Chapter 28
Anti-Virus 403

28.1 Anti-Virus Overview 403
28.1.1 Types of Computer Viruses 403
28.1.2 Computer Virus Infection and Prevention 403
28.1.3 Types of Anti-Virus Scanner 404
28.2 Introduction to the ZyWALL Anti-Virus Scanner 404
28.2.1 How the ZyWALL Anti-Virus Scanner Works 404
28.2.2 Notes About the ZyWALL Anti-Virus 405
28.3 Anti-Virus Summary 406
28.3.1 Anti-Virus Policy Edit 408
28.4 Anti-Virus Setting 410
28.5 Anti-Virus White List Add/Edit 412
28.6 Anti-Virus Black List Add/Edit 413
28.7 Signature Searching 413

Chapter 29
IDP 417

29.1 Introduction to IDP 417
29.1.1 Host Intrusions 417
29.1.2 Network Intrusions 417
29.1.3 IDP on the ZyWALL 417
29.1.4 Signatures 418
29.2 Traffic Directions and Profiles 418

29.3 Configuring IDP General 418
29.4 Configuring IDP Bindings 420
29.5 Introducing IDP Profiles 421
    29.5.1 Base Profiles 421
29.6 Profile Summary Screen 422
29.7 Creating New Profiles 423
    29.7.1 Procedure To Create a New Profile 423
29.8 Profiles: Packet Inspection 424
    29.8.1 Profile > Group View Screen 424
    29.8.2 Policy Types 427
    29.8.3 IDP Service Groups 428
    29.8.4 Profile > Query View Screen 429
    29.8.5 Query Example 431
29.9 Introducing IDP Custom Signatures 432
    29.9.1 IP Packet Header 432
29.10 Configuring Custom Signatures 434
    29.10.1 Creating or Editing a Custom Signature 435
    29.10.2 Custom Signature Example 439
    29.10.3 Applying Custom Signatures 442
    29.10.4 Verifying Custom Signatures 442
    29.10.5 Snort Signatures 443

Chapter 30
ADP 445

30.1 Introduction to ADP 445
    30.1.1 Host Intrusions 445
    30.1.2 Network Intrusions 445
    30.1.3 ADP on the ZyWALL 446
30.2 Traffic Directions and Profiles 446
30.3 Configuring ADP General 446
30.4 Configuring Anomaly Profile Bindings 447
30.5 Introducing ADP Profiles 448
    30.5.1 Base Profiles 448
30.6 Profile Summary Screen 449
30.7 Creating New Profiles 450
    30.7.1 Procedure To Create a New Profile 450
30.8 Profiles: Traffic Anomaly 450
    30.8.1 Port Scanning 451
    30.8.2 Flood Detection 452
    30.8.3 Profile > Traffic Anomaly Screen 455
30.9 Profiles: Protocol Anomaly 456
    30.9.1 HTTP Inspection and TCP/UDP/ICMP Decoders 457
    30.9.2 Protocol Anomaly Configuration 459

Chapter 31
Content Filter Screens..463

31.1 Content Filter Overview 463
31.1.1 Content Filter Policies 463
31.1.2 Content Filter Profiles 463
31.1.3 Content Filter Configuration Guidelines 464
31.2 Content Filter General Screen 464
31.3 Content Filter Policy Screen 466
31.4 Content Filter Profile Screen 467
31.5 External Web Filtering Service 468
31.6 Content Filter Categories Screen 469
31.7 Content Filter Customization Screen 477
31.8 Keyword Blocking URL Checking 480
31.9 Content Filter Cache Screen 480

Chapter 32
Content Filter Reports 483

32.1 Viewing Content Filter Reports 483
32.2 Web Site Submission 488

Part V: Device HA & Objects 491

Chapter 33
Device HA 493

33.1 Virtual Router Redundancy Protocol (VRRP) Overview 493
33.1.1 Additional VRRP Notes 495
33.2 VRRP Group Overview 495
33.2.1 Link Monitoring and Remote Management 496
33.3 Device HA Screens 496
33.4 VRRP Group Summary 496
33.5 VRRP Group Add/Edit 498
33.6 Synchronization Overview 500
33.6.1 Synchronization and Subscription Services 500
33.6.2 Synchronize Screen 501

Chapter 34
User/Group 503

34.1 User Account Overview 503
34.1.1 User Types 503
34.1.2 Ext-User Accounts 504
34.1.3 User Groups 505

34.1.4 Access Users and the ZyWALL 505
34.1.5 Force User Authentication Policy 505
34.2 User Summary 506
34.2.1 User Add/Edit 506
34.3 Group Summary 508
34.3.1 Group Add/Edit 509
34.4 Setting Screen 510
34.4.1 Force User Authentication Policy Add/Edit 512
34.5 Web Configurator for Non-Admin Users 513

Chapter 35
Addresses.......... 515

35.1 Addresses Overview 515
35.2 Address Screens 515
35.2.1 Address Summary 515
35.2.2 Address Add/Edit 516
35.3 Address Group Screens 517
35.3.1 Address Group Summary 517
35.3.2 Address Group Add/Edit 518

Chapter 36
Services 521

36.1 Services Overview 521
36.1.1 IP Protocols 521
36.1.2 Service Objects and Service Groups 521
36.2 Service Summary Screen 522
36.2.1 Service Add/Edit 523
36.3 Service Group Summary Screen 524
36.3.1 Service Group Add/Edit 524

Chapter 37
Schedules 527

37.1 Schedule Overview 527
37.2 Schedule Screens 527
37.2.1 Schedule Summary 527
37.2.2 One-Time Schedule Add/Edit 528
37.2.3 Recurring Schedule Add/Edit 529

Chapter 38
AAA Server 531

38.1 AAA Server Overview 531
38.1.1 ASAS 531
38.1.2 User Authentication Method 532

38.2 Directory Service (AD/LDAP) Overview 532
  38.2.1 Directory Structure 532
  38.2.2 Distinguished Name (DN) 533
  38.2.3 Configuring Active Directory or LDAP Default Server Settings 533
38.3 Active Directory or LDAP Group Summary 534
  38.3.1 Creating an Active Directory or LDAP Group 535
38.4 RADIUS Server 536
38.5 Configuring a Default RADIUS Server 537
38.6 Configuring a Group of RADIUS Servers 538
  38.6.1 Adding a RADIUS Server Member 538

Chapter 39
Authentication Objects..541

39.1 Authentication Objects Overview 541
39.2 Viewing Authentication Objects 541
39.3 Creating an Authentication Object 542
  39.3.1 Example: Selecting a VPN Authentication Method 543

Chapter 40
Certificates 545

40.1 Certificates Overview 545
  40.1.1 Advantages of Certificates 546
40.2 Self-signed Certificates 546
40.3 Factory Default Certificate 546
  40.3.1 Certificate File Formats 546
40.4 Certificate Configuration Screens Summary 547
40.5 Verifying a Certificate 547
  40.5.1 Checking the Fingerprint of a Certificate on Your Computer 547
40.6 My Certificates Screen 548
  40.6.1 My Certificates Add Screen 549
  40.6.2 My Certificate Edit Screen 552
  40.6.3 My Certificate Import Screen 555
40.7 Trusted Certificates Screen 556
  40.7.1 OCSP 556
40.8 Trusted Certificates Edit Screen 557
40.9 Trusted Certificates Import Screen 560

Chapter 41
ISP Accounts..563

41.1 ISP Accounts Overview 563
41.2 ISP Account Summary 563
41.3 ISP Account Edit 564

Chapter 42
SSL Application 567

42.1 SSL Application Overview 567
42.1.1 Application Types 567
42.1.2 Remote User Screen Links 567
42.2 SSL Application Configuration 567
42.3 Creating/Editing an SSL Application 568
42.3.1 Web-based Application 568
42.3.2 Example: Specifying a Web Site for Access 569
42.3.3 Configuring File Sharing 570

Part VI: System.. 573

Chapter 43
System 575

43.1 System Overview 575
43.2 Host Name 575
43.3 Time and Date 576
43.3.1 Pre-defined NTP Time Servers List 578
43.3.2 Time Server Synchronization 578
43.4 Console Port Speed 579
43.5 DNS Overview 580
43.5.1 DNS Server Address Assignment 580
43.5.2 DNS Servers 580
43.5.3 Configuring DNS 580
43.5.4 Address Record 583
43.5.5 PTR Record 583
43.5.6 Adding an Address/PTR Record 583
43.5.7 Domain Zone Forwarder 584
43.5.8 Adding a Domain Zone Forwarder 584
43.5.9 MX Record 585
43.5.10 Adding a MX Record 585
43.5.11 DNS Service Control 585
43.6 Language Screen 586

Chapter 44
Service Control 587

44.1 Service Control Overview 587
44.1.1 Service Access Limitations 588
44.1.2 System Timeout 588
44.2 HTTPS 588

44.3 Configuring WWW 589
44.4 Service Control Rules 592
44.5 HTTPS Example 592
    44.5.1 Internet Explorer Warning Messages 593
    44.5.2 Netscape Navigator Warning Messages 593
    44.5.3 Avoiding Browser Warning Messages 594
    44.5.4 Login Screen 595
    44.5.5 Enrolling and Importing SSL Client Certificates 595
    44.5.6 Using a Certificate When Accessing the ZyWALL Example 599
44.6 SSH 600
    44.6.1 How SSH Works 600
    44.6.2 SSH Implementation on the ZyWALL 601
    44.6.3 Requirements for Using SSH 601
    44.6.4 Configuring SSH 601
44.7 Secure Telnet Using SSH Examples 602
    44.7.1 Example 1: Microsoft Windows 602
    44.7.2 Example 2: Linux 603
44.8 Telnet 604
    44.8.1 Configuring Telnet 604
44.9 Configuring FTP 605
44.10 SNMP 606
    44.10.1 Supported MIBs 607
    44.10.2 SNMP Traps 607
    44.10.3 Configuring SNMP 608
44.11 Dial-in Management 609
    44.11.1 a managementAT Command Strings 609
    44.11.2 DTR Signal 609
    44.11.3 Response Strings 609
44.12 Dial-in Mgmt Configuration 609
44.13 Vantage CNM 610
44.14 Configuring Vantage CNM 611

Part VII: Maintenance & Troubleshooting 613

Chapter 45
File Manager 615

45.1 Configuration Files and Shell Scripts Overview 615
    45.1.1 Comments in Configuration Files or Shell Scripts 616
    45.1.2 Errors in Configuration Files or Shell Scripts 617
    45.1.3 ZyWALL Configuration File Details 617
    45.1.4 Configuration File Flow at Restart 617

45.2 Configuration File Screen 618
45.3 Firmware Package Screen 620
45.4 Shell Script Screen 622

Chapter 46
Logs 625

46.1 View Log Screen 625
46.2 Log Settings Screens 627
46.3 Log Settings Summary 628
46.3.1 Log Settings Edit E-mail 629
46.3.2 Log Settings Edit syslog 632
46.3.3 Active Log Summary 634

Chapter 47
Reports 637

47.1 Traffic Screen 637
47.2 Session Screen 640
47.3 Anti-Virus Report Screen 642
47.4 IDP Report Screen 643

Chapter 48
Diagnostics 647

48.1 Diagnostics 647

Chapter 49
Reboot 649

Chapter 50
Troubleshooting 651

50.1 Getting More Troubleshooting Help 652
50.2 Resetting the ZyWALL 652

Part VIII: Appendices and Index 655

Appendix A Product Specifications 657
Appendix B Log Descriptions 663
Appendix C Common Services 703
Appendix D Displaying Anti-Virus Alert Messages in Windows 707
Appendix E Importing Certificates 713

Appendix F Open Software Announcements 719

Appendix G Legal Information 755

Appendix H Customer Support.. 759

Index.. 765

List of Figures

Figure 1 ZyWALL USG 1000 Front Panel 53
Figure 2 Managing the ZyWALL: Web Configurator 54
Figure 3 Applications: VPN Connectivity 60
Figure 4 Network Access Mode: Reverse Proxy 61
Figure 5 Network Access Mode: Full Tunnel Mode 61
Figure 6 Applications: User-Aware Access Control 62
Figure 7 Applications: Multiple WAN Interfaces 62
Figure 8 Applications: Device HA 63
Figure 9 Login Screen 66
Figure 10 Update Admin Info Screen 66
Figure 11 Main Screen 67
Figure 12 Message Bar 72
Figure 13 Warning Messages 72
Figure 14 CLI Messages 73
Figure 15 Wizard Setup Welcome 76
Figure 16 Internet Access: Step 1 77
Figure 17 Ethernet Encapsulation: Auto: Finish 78
Figure 18 Ethernet Encapsulation: Static 79
Figure 19 Ethernet Encapsulation: Static: Finish 80
Figure 20 PPPoE Encapsulation: Auto 81
Figure 21 PPPoE Encapsulation: Auto: Finish 82
Figure 22 PPPoE Encapsulation: Static 83
Figure 23 PPPoE Encapsulation: Static: Finish 85
Figure 24 PPTP Encapsulation: Auto 86
Figure 25 PPTP Encapsulation: Auto: Finish 87
Figure 26 PPTP Encapsulation: Static 88
Figure 27 PPTP Encapsulation: Static: Finish 90
Figure 28 Registration 92
Figure 29 Registration: Registered Device 93
Figure 30 Internet Access: Step 1: First WAN Interface 94
Figure 31 Internet Access: Step 3: Second WAN Interface 94
Figure 32 Internet Access: Finish 95
Figure 33 VPN Wizard: Wizard Type 96
Figure 34 VPN Express Wizard: Step 2 97
Figure 35 VPN Express Wizard: Step 3 98
Figure 36 VPN Express Wizard: Step 4 99
Figure 37 VPN Express Wizard: Step 6 100
Figure 38 VPN Advanced Wizard: Step 2 102

Figure 39 VPN Advanced Wizard: Step 3 104
Figure 40 VPN Advanced Wizard: Step 4 106
Figure 41 VPN Advanced Wizard: Step 5 108
Figure 42 VPN Wizard: Step 6: Advanced 109
Figure 43 Interfaces and Zones: Example 114
Figure 44 Network > Interface > Port Grouping, Initial 126
Figure 45 Network > Interface > Port Grouping, Drag-and-Drop 126
Figure 46 Status: Interface Status Summary After Port Grouping 127
Figure 47 Network > Interface > Ethernet, Initial 127
Figure 48 Network > Interface > Ethernet > ge4 128
Figure 49 Network > Interface > Ethernet > ge5 > IP Address Assignment 128
Figure 50 Network > Interface > Ethernet > ge5 > DHCP Setting 128
Figure 51 Status > Interface Status Summary, After Ethernet Interface Edits 129
Figure 52 Network > Interface > Trunk, Initial 129
Figure 53 Network > Interface > Trunk > Edit, Initial 129
Figure 54 Network > Interface > Trunk > Edit > Member 130
Figure 55 Network > Zone, Initial 130
Figure 56 Network > Zone > DMZ, Remove ge4 131
Figure 57 Network > Zone > WAN, Add ge4 131
Figure 58 Status: Interface Status Summary After Zone Edits 131
Figure 59 VPN Example 132
Figure 60 VPN > IPSec VPN > VPN Gateway > Add 133
Figure 61 Object > Address > Address > Add 133
Figure 62 VPN > IPSec VPN > VPN Connection > add 134
Figure 63 Network > Routing > Policy Route 134
Figure 64 Network > Routing > Policy Route > Add 135
Figure 65 Network > Zone > Add 135
Figure 66 Device HA Example 136
Figure 67 Device HA > VRRP Group > Add: ge1 137
Figure 68 Status: Interface Status Summary: Device HA Master Configured 137
Figure 69 Network > Device HA > VRRP Group > Add: ge4 138
Figure 70 Device HA > Synchronize 138
Figure 71 Device HA > VRRP Group > Add 139
Figure 72 Status: Interface Status Summary 139
Figure 73 Device HA > Synchronize 140
Figure 74 User/Group > User > Add 141
Figure 75 User/Group > Group > Add 141
Figure 76 Object > AAA Server > RADIUS > Default 142
Figure 77 Object > Auth. method > Add 142
Figure 78 System > WWW > Authentication 142
Figure 79 Object > User/Group > Setting > Add (Force User Authentication Policy) 143
Figure 80 AppPatrol > http 143
Figure 81 AppPatrol > http > Edit Default 144

Figure 82 AppPatrol > http > Edit Default 144
Figure 83 Object > Schedule > Recurring > add 145
Figure 84 Firewall > LAN > DMZ > Edit 145
Figure 85 Firewall > LAN > DMZ > Add 146
Figure 86 Trunk Example 146
Figure 87 Network > Interface > Ethernet > Edit > ge2 147
Figure 88 Network > Interface > Trunk > WAN_TRUNK > Edit 147
Figure 89 NAT 1:1 Example Network Topology 148
Figure 90 Create Address Objects 148
Figure 91 Address Objects 148
Figure 92 NAT 1:1 Example Virtual Server 149
Figure 93 Create a Virtual Server 149
Figure 94 NAT 1:1 Example Policy Route 150
Figure 95 Create a Policy Route 150
Figure 96 Create a Firewall Rule 151
Figure 97 LAN Computer Queries the DNS Server 151
Figure 98 NAT Loopback Virtual Server 152
Figure 99 Create a Virtual Server 152
Figure 100 Triangle Route 153
Figure 101 NAT Loopback Policy Route 153
Figure 102 Create a Policy Route 154
Figure 103 NAT Loopback Successful 154
Figure 104 System > WWW 155
Figure 105 System > WWW > Service Control Rule Edit 156
Figure 106 System > WWW 156
Figure 107 Status 157
Figure 108 Status > VPN Status 161
Figure 109 Status > DHCP Table 162
Figure 110 Status > Port Statistics 163
Figure 111 Status > Current Users 164
Figure 112 Licensing > Registration 166
Figure 113 Licensing > Registration: Registered Device 168
Figure 114 Licensing > Registration > Service 168
Figure 115 Licensing > Update >Anti-Virus 172
Figure 116 Licensing > Update > IDP/AppPatrol 173
Figure 117 Downloading IDP Signatures 174
Figure 118 Successful IDP Signature Download 174
Figure 119 Licensing > Update > System Protect 175
Figure 120 Downloading System Protect Signatures 176
Figure 121 Successful System Protect Signature Download 176
Figure 122 Example: Entry in the Routing Table Derived from Interfaces 181
Figure 123 Network > Interface > Interface Summary 186
Figure 124 Network > Interface > Ethernet 188

Figure 125 Network > Interface > Ethernet > Edit 190
Figure 126 Network > Interface > Ethernet > Edit > Edit static DHCP table 194
Figure 127 Port Grouping Example: Network 195
Figure 128 Port Grouping Example: Screen 195
Figure 129 Network > Interface > Port Grouping 196
Figure 130 Example: Before VLAN 197
Figure 131 Example: After VLAN 197
Figure 132 Network > Interface > VLAN 198
Figure 133 Network > Interface > VLAN > Edit 200
Figure 134 Network > Interface > Edit > Edit static DHCP table 203
Figure 135 Network > Interface > Bridge 205
Figure 136 Network > Interface > Bridge > Edit 207
Figure 137 Network > Interface > Edit > Edit static DHCP table 210
Figure 138 Example: PPPoE/PPTP Interfaces 211
Figure 139 Network > Interface > PPPoE/PPTP 212
Figure 140 Network > Interface > PPPoE/PPTP > Edit 213
Figure 141 Network > Interface > Auxiliary 216
Figure 142 Network > Interface > Add 218
Figure 143 Least Load First Example 1 220
Figure 144 Weighted Round Robin Algorithm Example 221
Figure 145 Spillover Algorithm Example 222
Figure 146 Network > Interface > Trunk 222
Figure 147 Network > Interface > Trunk > Edit 223
Figure 148 Trigger Port Forwarding Example 227
Figure 149 Network > Routing > Policy Route 228
Figure 150 Network > Routing > Policy Route > Edit 230
Figure 151 Example of Static Routing Topology 232
Figure 152 Network > Routing > Static Route 233
Figure 153 Network > Routing > Static Route > Edit 233
Figure 154 Network > Routing > RIP 237
Figure 155 OSPF: Types of Areas 238
Figure 156 OSPF: Types of Routers 240
Figure 157 OSPF: Virtual Link 240
Figure 158 Network > Routing > OSPF 241
Figure 159 Network > Routing > OSPF > Edit 243
Figure 160 Example: Zones 245
Figure 161 Network > Zone 246
Figure 162 Network > Zone > Edit 247
Figure 163 Network > DDNS 251
Figure 164 Network > DDNS > Edit 252
Figure 165 Multiple Servers Behind NAT Example 256
Figure 166 Network > Virtual Server 257
Figure 167 Network > Virtual Server > Edit 258

Figure 168 HTTP Redirect Example 262
Figure 169 Network > HTTP Redirect 263
Figure 170 Network > HTTP Redirect > Edit 263
Figure 171 H.323 ALG Example 267
Figure 172 SIP ALG Example 267
Figure 173 VoIP Calls from the WAN with Multiple Outgoing Calls 268
Figure 174 VoIP with Multiple WAN IP Addresses 269
Figure 175 Network > ALG 269
Figure 176 WAN to LAN H.323 Peer-to-peer Calls Example 271
Figure 177 Network > Virtual Server > Add 271
Figure 178 Firewall > WAN to LAN 272
Figure 179 Firewall > WAN > LAN > Add 272
Figure 180 Object > Address > Add 272
Figure 181 Firewall > WAN > LAN > Add 273
Figure 182 Default Firewall Action 277
Figure 183 Blocking All LAN to WAN IRC Traffic Example 280
Figure 184 Limited LAN to WAN IRC Traffic Example 281
Figure 185 Triangle Route: Using Virtual Interfaces 283
Figure 186 Firewall 284
Figure 187 Firewall > Edit 286
Figure 188 Firewall Example: Select the Traveling Direction of Traffic 288
Figure 189 Firewall Example: Edit a Firewall Rule 1 288
Figure 190 Firewall Example: Create an Address Object 289
Figure 191 Firewall Example: Create a Service Object 289
Figure 192 Firewall Example: Edit a Firewall Rule 289
Figure 193 Firewall Example: MyService Example Rule in Summary 290
Figure 194 VPN: Example 291
Figure 195 VPN: IKE SA and IPSec SA 292
Figure 196 VPN: Transport and Tunnel Mode Encapsulation 293
Figure 197 VPN Example: NAT for Inbound and Outbound Traffic 295
Figure 198 VPN > IPSec VPN > VPN Connection 297
Figure 199 VPN > IPSec VPN > VPN Connection > Edit (IKE) 299
Figure 200 VPN > IPSec VPN > VPN Connection > Manual Key > Edit 303
Figure 201 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal 307
Figure 202 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange 308
Figure 203 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication 309
Figure 204 VPN/NAT Example 311
Figure 205 VPN > IPSec VPN > VPN Gateway 312
Figure 206 VPN > IPSec VPN > VPN Gateway > Edit 314
Figure 207 VPN Topologies 318
Figure 208 VPN > IPSec VPN > Concentrator 319
Figure 209 VPN > IPSec VPN > Concentrator > Edit 319
Figure 210 Network > IPSec VPN > Concentrator > Edit > Member 320

Figure 211 VPN > IPSec VPN > SA Monitor 321
Figure 212 VPN > SSL VPN > Access Privilege 324
Figure 213 VPN > SSL VPN > Access Privilege > Add/Edit 325
Figure 214 VPN > SSL VPN > Connection Monitor 327
Figure 215 VPN > SSL VPN > Global Setting 328
Figure 216 Example Logo Graphic Display 329
Figure 217 SSL VPN Client Portal Screen Example 330
Figure 218 Network Example 331
Figure 219 Enter the Address in a Web Browser 332
Figure 220 Login Security Screen 333
Figure 221 Login Screen 333
Figure 222 SecuExtender Progress 333
Figure 223 Remote User Screen 334
Figure 224 Add Favorite 335
Figure 225 Logout: Prompt 335
Figure 226 Logout: Connection Termination Progress 335
Figure 227 Application 337
Figure 228 File Sharing 340
Figure 229 File Sharing: Enter Access User Name and Password 340
Figure 230 File Sharing: Open a Word File 341
Figure 231 File Sharing: Save a Word File 342
Figure 232 File Sharing: Save a Word File 342
Figure 233 File Sharing: Rename 343
Figure 234 File Sharing: Rename 343
Figure 235 File Sharing: Delete Prompt 343
Figure 236 File Sharing: File Upload 344
Figure 237 L2TP VPN Overview 345
Figure 238 Policy Route for L2TP VPN 346
Figure 239 VPN > L2TP VPN 347
Figure 240 VPN > L2TP VPN > Session Monitor 348
Figure 241 L2TP VPN Example 351
Figure 242 VPN > IPSec VPN > VPN Gateway > Edit 352
Figure 243 VPN > IPSec VPN > VPN Gateway (Enable) 352
Figure 244 VPN > IPSec VPN > VPN Connection > Edit 353
Figure 245 VPN > IPSec VPN > VPN Connection (Enable) 354
Figure 246 VPN > L2TP VPN Example 354
Figure 247 Routing > Add: L2TP VPN Example 355
Figure 248 New Connection Wizard: Network Connection Type 356
Figure 249 New Connection Wizard: Network Connection 356
Figure 250 New Connection Wizard: Connection Name 357
Figure 251 New Connection Wizard: Public Network 357
Figure 252 New Connection Wizard: VPN Server Selection 358
Figure 253 Connect L2TP to ZyWALL 358

Figure 254 Connect L2TP to ZyWALL: Security 359
Figure 255 Connect ZyWALL L2TP: Security > Advanced 359
Figure 256 L2TP to ZyWALL Properties > Security 360
Figure 257 L2TP to ZyWALL Properties > Security > IPSec Settings 360
Figure 258 L2TP to ZyWALL Properties: Networking 360
Figure 259 Connect L2TP to ZyWALL 361
Figure 260 ZyWALL-L2TP System Tray Icon 361
Figure 261 ZyWALL-L2TP Status: Details 361
Figure 262 Starting the Registry Editor 362
Figure 263 Registry Key 362
Figure 264 New DWORD Value 362
Figure 265 ProhibitIpSec DWORD Value 363
Figure 266 Run mmc 363
Figure 267 Console > Add/Remove Snap-in 363
Figure 268 Add > IP Security Policy Management > Finish 364
Figure 269 Create IP Security Policy 364
Figure 270 IP Security Policy: Name 365
Figure 271 IP Security Policy: Request for Secure Communication 365
Figure 272 IP Security Policy: Completing the IP Security Policy Wizard 365
Figure 273 IP Security Policy Properties > Add 366
Figure 274 IP Security Policy Properties: Tunnel Endpoint 366
Figure 275 IP Security Policy Properties: Network Type 367
Figure 276 IP Security Policy Properties: Authentication Method 367
Figure 277 IP Security Policy Properties: IP Filter List 368
Figure 278 IP Security Policy Properties: IP Filter List > Add 368
Figure 279 Filter Properties: Addressing 369
Figure 280 Filter Properties: Protocol 369
Figure 281 IP Security Policy Properties: IP Filter List 370
Figure 282 IP Security Policy Properties: IP Filter List 370
Figure 283 Console: L2TP to ZyWALL Assign 370
Figure 284 Start New Connection Wizard 371
Figure 285 New Connection Wizard: Network Connection Type 371
Figure 286 New Connection Wizard: Destination Address 372
Figure 287 New Connection Wizard: Connection Availability 372
Figure 288 New Connection Wizard: Naming the Connection 372
Figure 289 Connect L2TP to ZyWALL 373
Figure 290 Connect L2TP to ZyWALL: Security 373
Figure 291 Connect L2TP to ZyWALL: Security > Advanced 374
Figure 292 Connect L2TP to ZyWALL: Networking 374
Figure 293 Connect L2TP to ZyWALL 375
Figure 294 ZyWALL-L2TP System Tray Icon 375
Figure 295 L2TP to ZyWALL Status: Details 375
Figure 296 LAN to WAN Connection and Packet Directions 381

Figure 297 LAN to WAN, Outbound 200 kbps, Inbound 500 kbps 382
Figure 298 Bandwidth Management Behavior 383
Figure 299 Application Patrol Bandwidth Management Example 385
Figure 300 SIP Any to WAN Bandwidth Management Example 386
Figure 301 HTTP Any to WAN Bandwidth Management Example 386
Figure 302 FTP WAN to DMZ Bandwidth Management Example 387
Figure 303 FTP LAN to DMZ Bandwidth Management Example 387
Figure 304 AppPatrol > General 389
Figure 305 AppPatrol > Common 390
Figure 306 Application Edit 391
Figure 307 Application Policy Edit 393
Figure 308 AppPatrol > Other 395
Figure 309 AppPatrol > Other > Edit 397
Figure 310 AppPatrol > Statistics: General Setup 399
Figure 311 AppPatrol > Statistics: Bandwidth Statistics 400
Figure 312 AppPatrol > Statistics: Protocol Statistics 401
Figure 313 ZyWALL Anti-virus Example 405
Figure 314 Anti-X > Anti-Virus > General 406
Figure 315 Anti-X > Anti-Virus > General > Edit 408
Figure 316 Anti-X > Anti-Virus > Setting 410
Figure 317 Anti-X > Anti-Virus > Setting > White List Add 412
Figure 318 Anti-X > Anti-Virus > Setting > Black List Add 413
Figure 319 Anti-X > Anti-Virus > Signature: Search by Severity 414
Figure 320 Anti-X > IDP > General 419
Figure 321 Anti-X > IDP > General > Add 421
Figure 322 Base Profiles 422
Figure 323 Anti-X > IDP > Profile 423
Figure 324 Anti-X > IDP > Profile > Edit : Group View 425
Figure 325 Anti-X > IDP > Profile > Edit > IDP Service Group 429
Figure 326 Anti-X > IDP > Profile: Query View 430
Figure 327 Query Example Search Criteria 431
Figure 328 Query Example Search Results 432
Figure 329 IP v4 Packet Headers 433
Figure 330 Anti-X > IDP > Custom Signatures 434
Figure 331 Anti-X > IDP > Custom Signatures > Add/Edit 436
Figure 332 Custom Signature Example Pattern 1 440
Figure 333 Custom Signature Example Pattern 2 440
Figure 334 Custom Signature Example Patterns 3 and 4 440
Figure 335 Example Custom Signature 441
Figure 336 Example: Custom Signature in IDP Profile 442
Figure 337 Custom Signature Log 443
Figure 338 Anti-X > ADP > General 446
Figure 339 Anti-X > ADP > General > Add 448

Figure 340 Base Profiles 449
Figure 341 Anti-X > ADP > Profile 449
Figure 342 Smurf Attack 452
Figure 343 TCP Three-Way Handshake 453
Figure 344 SYN Flood 453
Figure 345 Profiles: Traffic Anomaly 455
Figure 346 Profiles: Protocol Anomaly 460
Figure 347 Anti-X > Content Filter > General 464
Figure 348 Anti-X > Content Filter > General > Add I 466
Figure 349 Anti-X > Content Filter > Filter Profile 467
Figure 350 Content Filter Lookup Procedure 468
Figure 351 Anti-X > Content Filter > Filter Profile > Add 470
Figure 352 Anti-X > Content Filter > Filter Profile > Customization 478
Figure 353 Anti-X > Content Filter > Cache 481
Figure 354 myZyXEL.com: Login 483
Figure 355 myZyXEL.com: Welcome 484
Figure 356 myZyXEL.com: Service Management 484
Figure 357 Blue Coat: Login 485
Figure 358 Blue Coat Content Filter Reports Main Screen 485
Figure 359 Blue Coat: Report Home 486
Figure 360 Global Report Screen Example 487
Figure 361 Requested URLs Example 488
Figure 362 Web Page Review Process Screen 489
Figure 363 Example: VRRP, Normal Operation 493
Figure 364 Example: VRRP, Master Becomes Unavailable 494
Figure 365 Example: VRRP, No Preempt 494
Figure 366 Device HA > VRRP Group 497
Figure 367 Device HA > VRRP Group > Edit 498
Figure 368 Network > Device HA > Synchronize 501
Figure 369 LDAP Example: Keywords for User Attributes 504
Figure 370 RADIUS Example: Keywords for User Attributes 505
Figure 371 User/Group 506
Figure 372 User/Group > User > Edit 507
Figure 373 User/Group > Group 508
Figure 374 User/Group > Group > Add 509
Figure 375 User/Group > Setting 510
Figure 376 User/Group > Setting > Force User Authentication Policy > Add/Edit 512
Figure 377 Web Configurator for Non-Admin Users 513
Figure 378 Object > Address > Address 516
Figure 379 Object > Address > Address > Edit 516
Figure 380 Object > Address > Address Group 517
Figure 381 Object > Address > Address Group > Add 518
Figure 382 Object > Service > Service 522

Figure 383 Object > Service > Service > Edit 523
Figure 384 Object > Service > Service Group 524
Figure 385 Object > Service > Service Group > Edit 525
Figure 386 Object > Schedule 528
Figure 387 Object > Schedule > Edit (One Time) 529
Figure 388 Object > Schedule > Edit (Recurring) 530
Figure 389 Example: Directory Service Client and Server 532
Figure 390 Basic Directory Structure 533
Figure 391 Object > AAA Server > Active Directory (or LDAP) > Default 534
Figure 392 Object > AAA Server > Active Directory (or LDAP) > Group 535
Figure 393 Object > AAA Server > Active Directory (or LDAP) > Group > Add 535
Figure 394 RADIUS Server Network Example 537
Figure 395 Object > AAA Server > RADIUS > Default 537
Figure 396 Object > AAA Server > RADIUS > Group 538
Figure 397 Object > AAA Server > RADIUS > Group > Add 538
Figure 398 Object > Auth. Method 541
Figure 399 Object > Auth. Method > Add 542
Figure 400 Example: Using Authentication Method in VPN 544
Figure 401 Remote Host Certificates 547
Figure 402 Certificate Details 548
Figure 403 Object > Certificate > My Certificates 548
Figure 404 Object > Certificate > My Certificates > Add 550
Figure 405 Object > Certificate > My Certificates > Edit 553
Figure 406 Object > Certificate > My Certificates > Import 555
Figure 407 Object > Certificate > Trusted Certificates 556
Figure 408 Object > Certificate > Trusted Certificates > Edit 558
Figure 409 Object > Certificate > Trusted Certificates > Import 561
Figure 410 Object > ISP Account 563
Figure 411 Object > ISP Account > Edit 564
Figure 412 Object > SSL Application 567
Figure 413 Object > SSL Application > Add/Edit: Web Application 568
Figure 414 Example: SSL Application: Specifying a Web Site for Access 570
Figure 415 Object > SSL Application > Add/Edit: File Sharing 570
Figure 416 System > Host Name 575
Figure 417 System > Date and Time 576
Figure 418 Synchronization in Process 579
Figure 419 System > Console Port Speed 580
Figure 420 System > DNS 581
Figure 421 System > DNS > Address/PTR Record Edit 583
Figure 422 System > DNS > Domain Zone Forwarder Edit 584
Figure 423 System > DNS > MX Record Edit 585
Figure 424 System > DNS > Service Control Rule Edit 585
Figure 425 System > Language 586

Figure 426 Secure and Insecure Service Access From the WAN 587
Figure 427 HTTP/HTTPS Implementation 589
Figure 428 System > WWW 590
Figure 429 System > Service Control Rule Edit 592
Figure 430 Security Alert Dialog Box (Internet Explorer) 593
Figure 431 Security Certificate 1 (Netscape) 594
Figure 432 Security Certificate 2 (Netscape) 594
Figure 433 Login Screen (Internet Explorer) 595
Figure 434 ZyWALL Trusted CA Screen 595
Figure 435 CA Certificate Example 596
Figure 436 Personal Certificate Import Wizard 1 596
Figure 437 Personal Certificate Import Wizard 2 597
Figure 438 Personal Certificate Import Wizard 3 597
Figure 439 Personal Certificate Import Wizard 4 598
Figure 440 Personal Certificate Import Wizard 5 598
Figure 441 Personal Certificate Import Wizard 6 598
Figure 442 Access the ZyWALL Via HTTPS 599
Figure 443 SSL Client Authentication 599
Figure 444 Secure Web Configurator Login Screen 599
Figure 445 SSH Communication Over the WAN Example 600
Figure 446 How SSH v1 Works Example 600
Figure 447 System > SSH 601
Figure 448 SSH Example 1: Store Host Key 603
Figure 449 SSH Example 2: Test 603
Figure 450 SSH Example 2: Log in 603
Figure 451 System > Telnet 604
Figure 452 System > FTP 605
Figure 453 SNMP Management Model 606
Figure 454 System > SNMP 608
Figure 455 System > Dial-in Mgmt 610
Figure 456 System > Vantage CNM 611
Figure 457 Configuration File / Shell Script: Example 615
Figure 458 Maintenance > File Manager > Configuration File 618
Figure 459 Maintenance > File Manager > Configuration File > Copy 619
Figure 460 Maintenance > File Manager > Configuration File > Rename 619
Figure 461 Maintenance > File Manager > Firmware Package 621
Figure 462 Firmware Upload In Process 622
Figure 463 Network Temporarily Disconnected 622
Figure 464 Firmware Upload Error 622
Figure 465 Maintenance > File Manager > Shell Script 623
Figure 466 Maintenance > File Manager > Shell Script > Copy 623
Figure 467 Maintenance > File Manager > Shell Script > Rename 624
Figure 468 Maintenance > Log > View Log 626

Figure 469 Maintenance > Log > Log Setting 628
Figure 470 Maintenance > Log > Log Setting > E-mail > Edit 630
Figure 471 Maintenance > Log > Log Setting > Remote Server > Edit 633
Figure 472 Active Log Summary 635
Figure 473 Maintenance > Report > Traffic 638
Figure 474 Maintenance > Report > Session 641
Figure 475 Maintenance > Report > Anti-Virus: Virus Name 642
Figure 476 Maintenance > Report > Anti-Virus: Source 643
Figure 477 Maintenance > Report > Anti-Virus: Destination 643
Figure 478 Maintenance > Report > IDP: Signature Name 644
Figure 479 Maintenance > Report > IDP: Source 645
Figure 480 Maintenance > Report > IDP: Destination 645
Figure 481 Maintenance > Diagnostics 647
Figure 482 Maintenance > Reboot 649
Figure 483 Windows XP: Opening the Services Window 707
Figure 484 Windows XP: Starting the Messenger Service 708
Figure 485 Windows 2000: Opening the Services Window 708
Figure 486 Windows 2000: Starting the Messenger Service 709
Figure 487 Windows 98 SE: WinPopup 709
Figure 488 WIndows 98 SE: Program Task Bar 709
Figure 489 Windows 98 SE: Task Bar Properties 710
Figure 490 Windows 98 SE: StartUp 710
Figure 491 Windows 98 SE: Startup: Create Shortcut 711
Figure 492 Windows 98 SE: Startup: Select a Title for the Program 711
Figure 493 Windows 98 SE: Startup: Shortcut 712
Figure 494 Security Certificate 713
Figure 495 Login Screen 714
Figure 496 Certificate General Information before Import 714
Figure 497 Certificate Import Wizard 1 715
Figure 498 Certificate Import Wizard 2 715
Figure 499 Certificate Import Wizard 3 716
Figure 500 Root Certificate Store 716
Figure 501 Certificate General Information after Import 717

List of Tables

Table 1 Front Panel LEDs 54
Table 2 Managing the ZyWALL: Console Port 55
Table 3 Starting and Stopping the ZyWALL 55
Table 4 Packet Flow Key 58
Table 5 Title Bar: Web Configurator Icons 68
Table 6 Navigation Panel Summary 68
Table 7 Internet Access: Step 1 77
Table 8 Ethernet Encapsulation: Static 79
Table 9 PPPoE Encapsulation: Auto 81
Table 10 PPPoE Encapsulation: Static 83
Table 11 PPTP Encapsulation: Auto 86
Table 12 PPTP Encapsulation: Static 88
Table 13 Registration 92
Table 14 VPN Wizard: Step 1: Wizard Type 96
Table 15 VPN Express Wizard: Step 2 97
Table 16 VPN Express Wizard: Step 3 98
Table 17 VPN Express Wizard: Step 4 99
Table 18 VPN Advanced Wizard: Step 2 102
Table 19 VPN Advanced Wizard: Step 3 104
Table 20 VPN Advanced Wizard: Step 4 106
Table 21 VPN Advanced Wizard: Step 5 108
Table 22 ZyWALL Terminology That is Different Than ZyNOS 112
Table 23 ZyWALL Terminology That Might Be Different Than Other Products 112
Table 24 NAT: Differences Between the ZyWALL and ZyNOS 112
Table 25 Bandwidth Management: Differences Between the ZyWALL and ZyNOS 112
Table 26 Physical Ports, Interfaces, and Zones 112
Table 27 Objects 122
Table 28 User Types 122
Table 29 Interfaces and Zones Example 125
Table 30 Ethernet Interfaces Example 127
Table 31 Trunk Example 129
Table 32 Zones Example 130
Table 33 User-Aware Access Control Example 140
Table 34 Status 158
Table 35 Status > VPN Status 161
Table 36 Status > DHCP Table 162
Table 37 Status > Port Statistics 163
Table 38 Status > Current Users 164

Table 39 Licensing > Registration 167
Table 40 Licensing > Registration > Service 168
Table 41 Licensing > Update > IDP/AppPatrol 173
Table 42 Licensing > Update > System Protect 175
Table 43 Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interfaces Characteristics 180
Table 44 Example: Routing Table Entries for Interfaces 181
Table 45 Example: Routing Table Entry for a Gateway 181
Table 46 Example: Assigning IP Addresses from a Pool 182
Table 47 Relationships Between Different Types of Interfaces 184
Table 48 Network > Interface > Interface Summary 186
Table 49 Network > Interface > Ethernet 189
Table 50 Network > Interface > Ethernet > Edit 191
Table 51 Network > Interface > Port Grouping 196
Table 52 Network > Interface > VLAN 198
Table 53 Network > Interface > VLAN > Edit 201
Table 54 Example: Bridge Table After Computer A Sends a Packet to Computer B 204
Table 55 Example: Bridge Table After Computer B Responds to Computer A 204
Table 56 Example: Routing Table Before and After Bridge Interface br0 Is Created 205
Table 57 Network > Interface > Bridge 205
Table 58 Network > Interface > Bridge > Edit 208
Table 59 Network > Interface > PPPoE/PPTP 212
Table 60 Network > Interface > PPPoE/PPTP > Edit 214
Table 61 Network > Interface > Auxiliary 216
Table 62 Network > Interface > Add 218
Table 63 Least Load First: Example 1 220
Table 64 Network > Interface > Trunk 222
Table 65 Network > Interface > Trunk > Edit 223
Table 66 Network > Routing > Policy Route 228
Table 67 Network > Routing > Policy Route > Edit 230
Table 68 Network > Routing > Static Route 233
Table 69 Network > Routing > Static Route > Edit 234
Table 70 OSPF vs. RIP 235
Table 71 Network > Routing Protocol > RIP 237
Table 72 OSPF: Redistribution from Other Sources to Each Type of Area 239
Table 73 Network > Routing Protocol > OSPF 241
Table 74 Network > Routing > OSPF > Edit 243
Table 75 Network > Zone 246
Table 76 Network > Zone > Edit 247
Table 77 Network > DDNS 251
Table 78 Network > DDNS > Edit 252
Table 79 Network > Virtual Server 257
Table 80 Network > Virtual Server > Edit 258
Table 81 Network > HTTP Redirect 263

Table 82 Network > HTTP Redirect > Edit 263
Table 83 Network > ALG 270
Table 84 Default Firewall Rules 279
Table 85 Blocking All LAN to WAN IRC Traffic Example 281
Table 86 Limited LAN to WAN IRC Traffic Example 1 282
Table 87 Limited LAN to WAN IRC Traffic Example 2 282
Table 88 Firewall 284
Table 89 Firewall > Edit 286
Table 90 VPN > IPSec VPN > VPN Connection 298
Table 91 VPN > IPSec VPN > VPN Connection > Edit 299
Table 92 VPN > IPSec VPN > VPN Connection > Manual Key > Edit 303
Table 93 VPN Example: Matching ID Type and Content 310
Table 94 VPN Example: Mismatching ID Type and Content 310
Table 95 VPN > IPSec VPN > VPN Gateway 312
Table 96 VPN > IPSec VPN > VPN Gateway > Edit 314
Table 97 VPN > IPSec VPN > Concentrator 319
Table 98 VPN > IPSec VPN > Concentrator > Edit 320
Table 99 VPN > IPSec VPN > SA Monitor 321
Table 100 Objects 323
Table 101 VPN > SSL VPN > Access Privilege 324
Table 102 VPN > SSL VPN > Access Privilege > Add/Edit 325
Table 103 VPN > SSL VPN > Connection Monitor 327
Table 104 VPN > SSL VPN > Global Setting 328
Table 105 Remote User Screen Overview 334
Table 106 VPN > IPSec VPN > VPN Connection 347
Table 107 VPN > L2TP VPN > Session Monitor 348
Table 108 Configured Rate Effect 383
Table 109 Priority Effect 383
Table 110 Maximize Bandwidth Usage Effect 383
Table 111 Priority and Over Allotment of Bandwidth Effect 384
Table 112 AppPatrol > General 389
Table 113 AppPatrol > Common 390
Table 114 Application Edit 391
Table 115 Application Policy Edit 393
Table 116 AppPatrol > Other 396
Table 117 AppPatrol > Other > Edit 397
Table 118 AppPatrol > Statistics: General Setup 400
Table 119 AppPatrol > Statistics: Protocol Statistics 401
Table 120 Common Computer Virus Types 403
Table 121 Anti-X > Anti-Virus > General 407
Table 122 Anti-X > Anti-Virus > General > Edit 408
Table 123 Anti-X > Anti-Virus > Setting 411
Table 124 Anti-X > Anti-Virus > Setting > White List Add 412

Table 125 Anti-X > Anti-Virus > Setting > Black List Add 413
Table 126 Anti-X > Anti-Virus > Signature 414
Table 127 Anti-X > IDP > General 419
Table 128 Anti-X > IDP > General > Add 421
Table 129 Base Profiles 422
Table 130 Anti-X > IDP > Profile 423
Table 131 Anti-X > IDP > Profile > Group View 426
Table 132 Policy Types 427
Table 133 IDP Service Groups 428
Table 134 Anti-X > IDP > Profile: Query View 430
Table 135 IP v4 Packet Headers 433
Table 136 Anti-X > IDP > Custom Signatures 435
Table 137 Anti-X > IDP > Custom Signatures > Add/Edit 437
Table 138 ZyWALL - Snort Equivalent Terms 443
Table 139 Anti-X > ADP > General 447
Table 140 Anti-X > ADP > General > Add 448
Table 141 Base Profiles 449
Table 142 Anti-X > ADP > Profile 449
Table 143 ADP > Profile > Traffic Anomaly 456
Table 144 HTTP Inspection and TCP/UDP/ICMP Decoders 457
Table 145 ADP > Profile > Protocol Anomaly 461
Table 146 Anti-X > Content Filter > General 464
Table 147 Anti-X > Content Filter > General > Add 467
Table 148 Anti-X > Content Filter > Filter Profile 467
Table 149 Anti-X > Content Filter > Filter Profile > Add 470
Table 150 Anti-X > Content Filter > Filter Profile > Customization 478
Table 151 Anti-X > Content Filter > Cache 481
Table 152 Device HA > VRRP Group 497
Table 153 Device HA > VRRP Group > Edit 498
Table 154 Network > Device HA > Synchronize 501
Table 155 Types of User Accounts 503
Table 156 LDAP/RADIUS: Keywords for User Attributes 504
Table 157 User/Group 506
Table 158 User/Group > User > Edit 507
Table 159 Reserved User Names 508
Table 160 User/Group > Group 508
Table 161 User/Group > Group > Add 509
Table 162 User/Group > Setting 510
Table 163 User/Group > Setting > Force User Authentication Policy > Add/Edit 513
Table 164 Web Configurator for Non-Admin Users 514
Table 165 Object > Address > Address 516
Table 166 Object > Address > Address > Edit 517
Table 167 Object > Address > Address Group 518

Table 168 Object > Address > Address Group > Add 518
Table 169 Object > Service > Service 522
Table 170 Object > Service > Service > Edit 523
Table 171 Object > Service > Service Group 524
Table 172 Object > Service > Service Group > Edit 525
Table 173 Object > Schedule 528
Table 174 Object > Schedule > Edit (One Time) 529
Table 175 Object > Schedule > Edit (Recurring) 530
Table 176 Object > AAA Server > Active Directory (or LDAP) > Default 534
Table 177 Object > AAA Server > Active Directory (or LDAP) > Group 535
Table 178 Object > AAA Server > Active Directory (or LDAP) > Group > Add 536
Table 179 Object > AAA Server > RADIUS > Default 537
Table 180 Object > AAA Server > RADIUS > Group 538
Table 181 Object > AAA Server > RADIUS > Group > Add 539
Table 182 Object > Auth. Method 541
Table 183 Object > Auth. Method > Add 543
Table 184 Object > Certificate > My Certificates 549
Table 185 Object > Certificate > My Certificates > Add 550
Table 186 Object > Certificate > My Certificates > Edit 553
Table 187 Object > Certificate > My Certificates > Import 556
Table 188 Object > Certificate > Trusted Certificates 556
Table 189 Object > Certificate > Trusted Certificates > Edit 558
Table 190 Object > Certificate > Trusted Certificates > Import 561
Table 191 Object > ISP Account 563
Table 192 Object > ISP Account > Edit 564
Table 193 Object > SSL Application 568
Table 194 Object > SSL Application > Add/Edit: Web Application 569
Table 195 Object > SSL Application > Add/Edit: Web Application 570
Table 196 System > Host Name 575
Table 197 System > Date and Time 576
Table 198 Default Time Servers 578
Table 199 System > Console Port Speed 580
Table 200 System > DNS 581
Table 201 System > DNS > Address/PTR Record Edit 583
Table 202 System > DNS > Domain Zone Forwarder Edit 584
Table 203 System > DNS > MX Record Edit 585
Table 204 System > DNS > Service Control Rule Edit 586
Table 205 System > Language 586
Table 206 System > WWW 590
Table 207 Edit Service Control Rule 592
Table 208 System > SSH 602
Table 209 System > Telnet 604
Table 210 System > FTP 605

Table 211 SNMP Traps 607
Table 212 System > SNMP 608
Table 213 System > Dial-in Mgmt 610
Table 214 System > Vantage CNM 611
Table 215 Configuration Files and Shell Scripts in the ZyWALL 616
Table 216 Maintenance > File Manager > Configuration File 619
Table 217 Maintenance > File Manager > Firmware Package 621
Table 218 Maintenance > File Manager > Shell Script 623
Table 219 Specifications: Logs 625
Table 220 Maintenance > Log > View Log 626
Table 221 Maintenance > Log > Log Setting 628
Table 222 Maintenance > Log > Log Setting > E-mail > Edit 631
Table 223 Maintenance > Log > Log Setting > Remote Server > Edit 634
Table 224 Maintenance > Log > Log Setting > Active Log Summary 635
Table 225 Maintenance > Report > Traffic 638
Table 226 Maximum Values for Reports 640
Table 227 Maintenance > Report > Session 641
Table 228 Maintenance > Report > Anti-Virus 642
Table 229 Maintenance > Report > IDP 644
Table 230 Maintenance > Diagnostics 647
Table 231 Default Login Information 657
Table 232 Hardware Specifications 657
Table 233 Feature Specifications 658
Table 234 Standards Referenced by Features 660
Table 235 Content Filter Logs 663
Table 236 Forward Web Site Logs 663
Table 237 Blocked Web Site Logs 663
Table 238 User Logs 665
Table 239 myZyXEL.com Logs 666
Table 240 IDP Logs 670
Table 241 Application Patrol Logs 673
Table 242 IKE Logs 675
Table 243 IPSec Logs 679
Table 244 Firewall Logs 680
Table 245 Sessions Limit Logs 680
Table 246 Policy Route Logs 680
Table 247 Built-in Services Logs 682
Table 248 System Logs 685
Table 249 Connectivity Check Logs 689
Table 250 Device HA Logs 690
Table 251 Routing Protocol Logs 693
Table 252 NAT Logs 695
Table 253 PKI Logs 696

Table 254 Interface Logs 699
Table 255 Account Logs 701
Table 256 Port Grouping Logs 701
Table 257 Force Authentication Logs 702
Table 258 File Manager Logs 702
Table 259 Commonly Used Services 703

PART I

Introduction

Introducing the ZyWALL (53)
Features and Applications (57)
Web Configurator (65)
Configuration Basics (111)
Tutorials (125)
Status (157)
Registration (165)
Update (171)

1

Introducing the ZyWALL

This chapter gives an overview of the ZyWALL. It explains the front panel ports, LEDs, introduces the management methods, and lists different ways to start or stop the ZyWALL.

1.1 Overview and Key Default Settings

The ZyWALL is an Internet Security Gateway designed for Small and Medium Businesses (SMB). Its flexible configuration helps network administrators set up the network and enforce security policies efficiently. In addition, the ZyWALL provides excellent throughput, making it an ideal solution for reliable, secure service.

The physical ports on the front panel of the ZyWALL are called “ge1”, “ge2”, “ge3”, and so on where “ge” stands for Gigabit Ethernet. By default “ge1” is mapped to port 1, “ge2” to port 2 and so on.

Also, by default “ge1” is the LAN interface, “ge2” and “ge3” are combined as the WAN_TRUNK. See Section 50.2 on page 652 for how to use the **RESET** button.

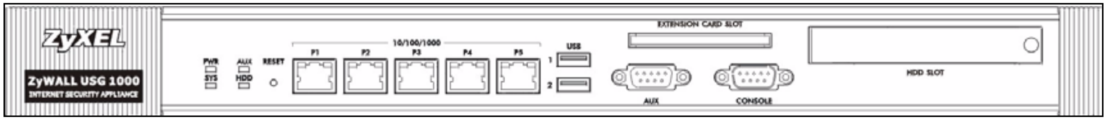
The Ethernet management interface can only be accessed from LAN side by default. The default management IP address is 192.168.1.1; the default login user name and password are “admin” and “1234” respectively.

To enable management access from the WAN, log into the web configurator, go to **System** > **WWW**, and change the default **Deny** to **Accept** in the rule in the **Admin Service Control** section.

You should configure the **Network** > **Interface** screens first to establish network connectivity before configuring security features such as firewall, VPN, content filtering, IDP and so on.

1.2 Front Panel LEDs

Figure 1 ZyWALL USG 1000 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ZyWALL is turned off.
	Green	On	The ZyWALL is turned on.
	Red	On	There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device (see Section 1.4 on page 55). If the LED turns red again, then please contact your vendor.
SYS	Green	Off	The ZyWALL is not ready or has failed.
		On	The ZyWALL is ready and running.
		Flashing	The ZyWALL is restarting.
AUX	Green	Off	The **AUX** port is not connected.
		Flashing	The **AUX** port is sending or receiving packets.
		On	The **AUX** port is connected.
HDD	Green	Off	Reserved for future use. No hard disk is present. The ZyWALL can run without the hard disk.
		On	The hard disk is present.
		Flashing	The ZyWALL is accessing the hard disk.
P1 ~ P5	Green	Off	There is no traffic on this port.
		Flashing	The ZyWALL is sending or receiving packets on this port.
	Orange	Off	There is no connection on this port.
		On	This port has a successful link.

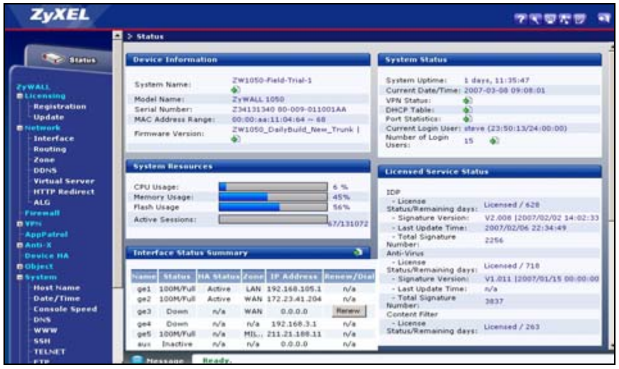
1.3 Management Overview

You can use the following ways to manage the ZyWALL.

Web Configurator

The web configurator allows easy ZyWALL setup and management using an Internet browser. This User's Guide provides information about the web configurator.

Figure 2 Managing the ZyWALL: Web Configurator



ZyXEL
Status
Status
ZyWALL
Licensing
Registration
Update
Network
Interface
Routing
Zone
DDNS
Virtual Server
HTTP Redirect
ALG
Firewall
VPN
AppPatrol
Anti-X
Device HA
Object
System
Host Name
Date/Time
Console Speed
DNS
WWW
SSH
TELNET
FTP
Device Information
System Status
System Resources
Licensed Service Status
Interface Status Summary
Renew
Message

System Name: ZW1050-Field-Trial-1
Model Name: ZyWALL 1050
Serial Number: Z34131340 00-009-011001AA
MAC Address Range: 00:00:aa:11:04:64 ~ 68
Firmware Version: ZW1050_DailyBuild_New_Trunk |

System Uptime: 1 days, 11:35:47
Current Date/Time: 2007-03-08 09:08:01
VPN Status:
DHCP Table:
Port Statistics:
Current Login User: steve (23:50:13/24:00:00)
Number of Login Users: 15

CPU Usage: 6 %
Memory Usage: 45%
Flash Usage 56%
Active Sessions: 67/131072

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	100M/Full	Active	LAN	192.168.105.1	n/a
ge2	100M/Full	Active	WAN	172.23.41.204	n/a
ge3	Down	n/a	WAN	0.0.0.0	Renew
ge4	Down	n/a	n/a	192.168.3.1	n/a
ge5	100M/Full	n/a	MIL...	211.21.188.11	n/a
aux	Inactive	n/a	n/a	0.0.0.0	n/a

IDP
- License Status/Remaining days: Licensed / 628
- Signature Version: V2.008 |2007/02/02 14:02:33
- Last Update Time: 2007/02/06 22:34:49
- Total Signature Number: 2256

Anti-Virus
- License Status/Remaining days: Licensed / 718
- Signature Version: V1.011 |2007/01/15 00:00:00
- Last Update Time: n/a
- Total Signature Number: 3837

Content Filter
- License Status/Remaining days: Licensed / 263

Ready.

Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the ZyWALL. You can access it using remote management (for example, SSH or Telnet) or via the console port. See the Command Reference Guide for more information about the CLI.

Console Port

You can use the console port to manage the ZyWALL. You have to use CLI commands, which are explained in the Command Reference Guide.

The default settings for the console port are as follows.

Table 2 Managing the ZyWALL: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

1.4 Starting and Stopping the ZyWALL

This section explains some of the ways to start and stop the ZyWALL. These are summarized below.

Table 3 Starting and Stopping the ZyWALL

METHOD	DESCRIPTION
Turning on the power button	A cold start occurs when you turn on the power to the ZyWALL. The ZyWALL powers up, checks the hardware, and starts the system processes.
Rebooting the ZyWALL	A warm start (without powering down and powering up again) occurs when you use the **Reboot** button in the **Reboot** screen or when you use the `reboot` command. The ZyWALL writes all cached data to disk, stops the system processes, and then does a warm start.
Using the RESET button	If you press the **RESET** button, the ZyWALL sets the configuration to its default values and then reboots.
Using the `shutdown` command	The `shutdown` command writes all cached data to disk and stops the system processes. It does not turn off the power.You have to turn the power off and on manually to start the ZyWALL again. You should use this command before you turn off the ZyWALL.
Turning off the power button	Power off occurs when you turn off the power to the ZyWALL. The ZyWALL simply turns off. It does not stop the system processes or write cached data to disk.

It is recommended you use the `shutdown` command before turning off the ZyWALL.

When you apply configuration files or running shell scripts, the ZyWALL does not stop or start the system processes. However, you might lose access to network resources temporarily while the ZyWALL is applying configuration files or running shell scripts.

2

Features and Applications

This chapter introduces the main features and applications of the ZyWALL.

2.1 Features

The ZyWALL's security features include VPN, firewall, anti-virus, content filtering, IDP (Intrusion Detection and Prevention), ADP (Anomaly Detection and Protection), and certificates. It also provides bandwidth management, NAT, port forwarding, policy routing, DHCP server and many other powerful features.

The rest of this section provides more information about the features of the ZyWALL.

High Availability

To ensure the ZyWALL provides reliable, secure Internet access, set up one or more of the following:

- Multiple WAN ports and configure load balancing between these ports
- A backup Internet connection
- A backup ZyWALL in the event the master ZyWALL fails (device HA).

Virtual Private Networks (VPN)

Use IPSec, SSL, or L2TP VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ZyWALL also offers hub-and-spoke IPSec VPN.

Flexible Security Zones

Many security settings are made by zone, not by interface, port, or network. As a result, it is much simpler to set up and to change security settings in the ZyWALL. You can create or remove zones, and you can assign each network, VLAN, or interface to any zone.

Firewall

The ZyWALL's firewall is a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Intrusion Detection and Prevention (IDP)

IDP (Intrusion Detection and Protection) can detect malicious or suspicious packets and respond instantaneously. It detects pattern-based attacks in order to protect against network-based intrusions. See Section 29.8.2 on page 427 for a list of attacks that the ZyWALL can protect against. You can also create your own custom IDP rules.

Anomaly Detection and Prevention (ADP)

ADP (Anomaly Detection and Prevention) can detect malicious or suspicious packets and respond instantaneously. It can detect:

- Anomalies based on violations of protocol standards (RFCs – Requests for Comments)
- Abnormal flows such as port scans.

The ZyWALL’s ADP protects against network-based intrusions. See Section 30.8 on page 450 and Section 30.9 on page 456 for more on the kinds of attacks that the ZyWALL can protect against. You can also create your own custom ADP rules.

Bandwidth Management

Bandwidth management allows you to allocate network resources according to defined policies. This policy-based bandwidth allocation helps your network to better handle applications such as Internet access, e-mail, Voice-over-IP (VoIP), video conferencing and other business-critical applications.

Content Filter

Content filtering allows schools and businesses to create and enforce Internet access policies tailored to the needs of the organization.

You can also subscribe to category-based content filtering that allows your ZyWALL to check web sites against an external database of dynamically-updated ratings of millions of web sites. You then simply select categories to block or monitor, such as pornography or racial intolerance, from a pre-defined list.

Anti-Virus Scanner

With the anti-virus packet scanner, your ZyWALL scans files transmitting through the enabled interfaces into the network. The ZyWALL helps stop threats at the network edge before they reach the local host computers.

2.2 Packet Flow

The following is the key used to describe the packet flow in the ZyWALL.

Table 4 Packet Flow Key

Ethernet	The interface on which the packet is received or sent
VLAN	Virtual LAN
Encap	The PPPoE or PPTP encapsulation used
ALG	Application Layer Gateway

Table 4 Packet Flow Key

AC	Application Classifier is the Application Protocol (AP) layer-7 classifier.
DNAT	Destination NAT
Routing	Routing includes policy routes, interface routing, static routes and load balancing for example.
FW	Firewall (Through ZyWALL)
zFW	Firewall (To ZyWALL)
IDP	Intrusion Detection & Protection
ADP	Anomaly Detection and Protection
AP	Application Patrol
CF	Content Filtering
SNAT	Source NAT
IPSec D/E	VPN Decryption/Encryption
BWM	Bandwidth Management
RM	Remote Management (System)
AV	Anti-Virus

2.2.1 Interface to Interface (Through ZyWALL)

Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT-> Routing -> FW -> AC -> IDP -> AV-> AP -> CF -> SNAT -> BWM -> Encap -> VLAN -> Ethernet

2.2.2 Interface to Interface (To/From ZyWALL)

To: Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT -> Routing -> zFW -> ADP -> RM
From: RM -> Routing -> BWM -> Encap -> VLAN -> Ethernet

2.2.3 Interface to Interface (From VPN Tunnel)

This example shows the flow from a VPN tunnel though the ZyWALL, not to the ZyWALL or to another VPN tunnel (VPN concentrator).

Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT-> Routing -> zFW -> IPSec D -> ALG -> AC -> DNAT-> Routing -> FW -> AC -> IDP -> AV -> AP -> CF -> -> SNAT -> BWM -> Encap -> VLAN -> Ethernet

2.2.4 Interface to Interface (To VPN Tunnel)

This example shows the flow to a VPN tunnel from a source other than the ZyWALL or another VPN tunnel (VPN concentrator).

Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT-> Routing -> FW -> AC -> IDP -> AV -> AP -> CF -> SNAT -> IPSec E -> Routing -> BWM -> Encap -> VLAN -> Ethernet

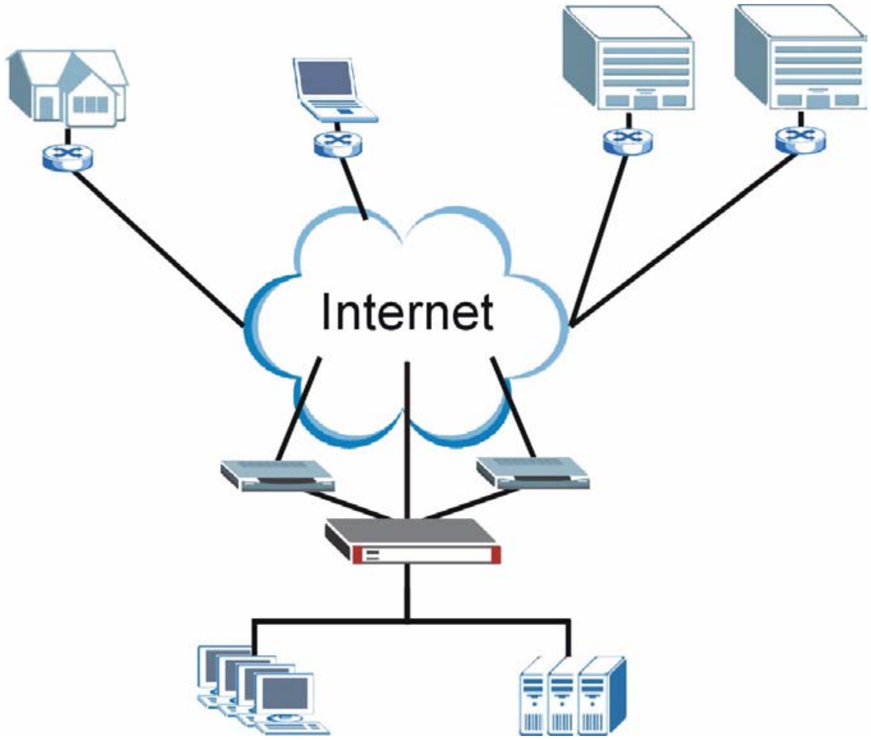
2.3 Applications

These are some example applications for your ZyWALL. See also Chapter 6 on page 125 for configuration tutorial examples.

2.3.1 VPN Connectivity

Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. You can also set up additional connections to the Internet to provide better service.

Figure 3 Applications: VPN Connectivity



2.3.2 SSL VPN Network Access

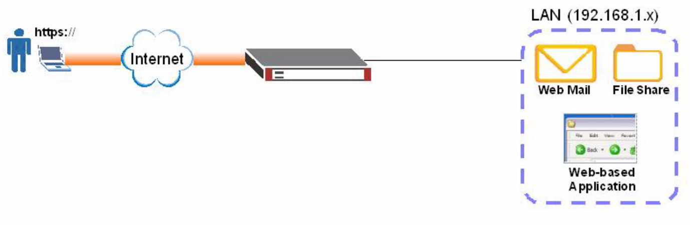
You can configure the ZyWALL to provide SSL VPN network access to remote users. There are two SSL VPN network access modes: reverse proxy and full tunnel.

2.3.2.1 Reverse Proxy Mode

In reverse proxy mode, the ZyWALL is a proxy that acts on behalf of the local network servers (such as your web and mail servers). As the final destination, the ZyWALL appears to be the server to remote users. This provides an added layer of protection for your internal servers.

With reverse proxy mode, remote users can easily access any web-based applications on the local network by clicking on links or entering the provided URL. You do not have to install additional client software on the remote user computers for access.

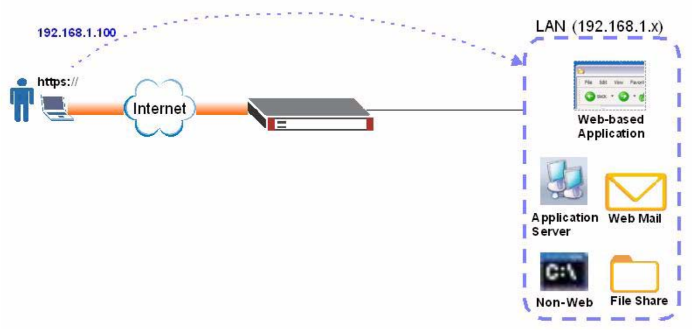
Figure 4 Network Access Mode: Reverse Proxy


LAN (192.168.1.x)
https://
Internet
Web Mail
File Share
Web-based Application

2.3.2.2 Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

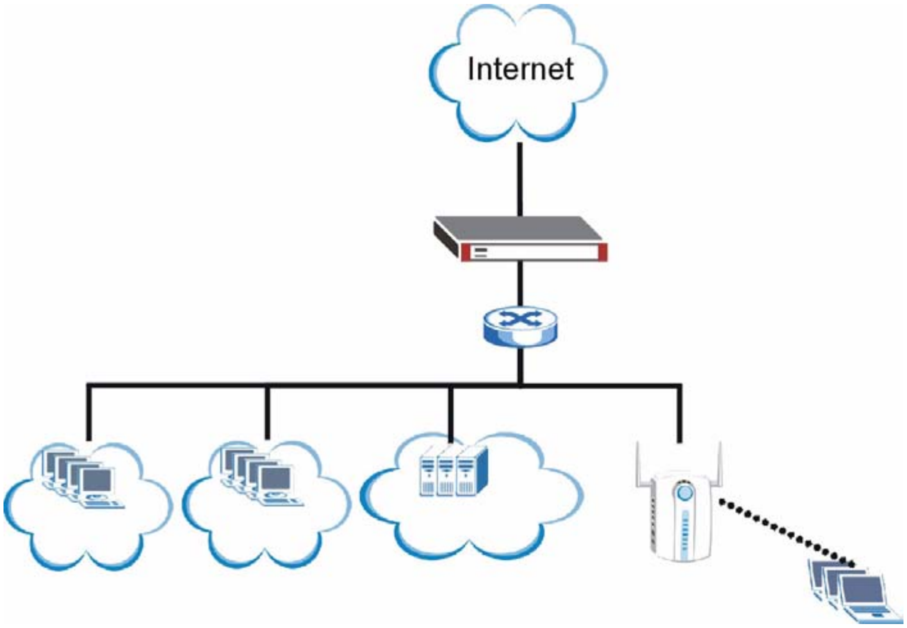
Figure 5 Network Access Mode: Full Tunnel Mode


192.168.1.100
LAN (192.168.1.x)
https://
Internet
Web-based Application
Application Server
Web Mail
Non-Web
File Share

2.3.3 User-Aware Access Control

Set up security policies that restrict access to sensitive information and shared resources based on the user who is trying to access it.

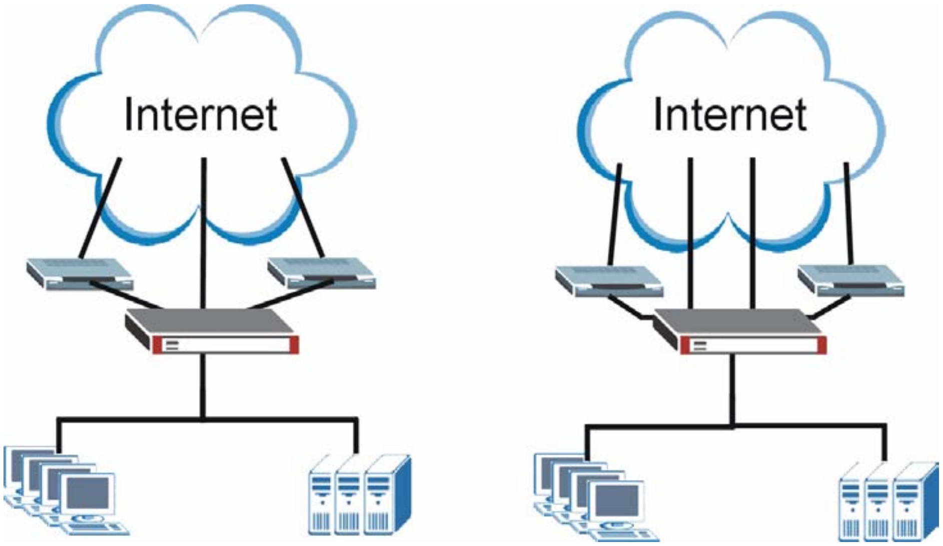
Figure 6 Applications: User-Aware Access Control



2.3.4 Multiple WAN Interfaces

Set up multiple connections to the Internet on the same port, or set up multiple connections on different ports. In either case, you can balance the loads between them.

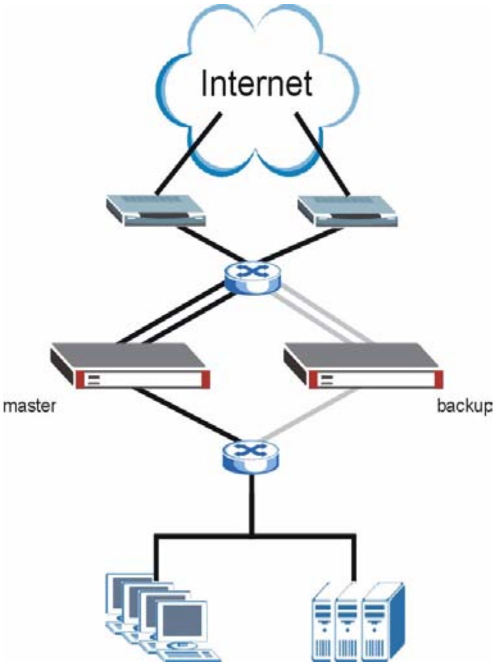
Figure 7 Applications: Multiple WAN Interfaces



2.3.5 Device HA

Set up an additional ZyWALL as a backup gateway to ensure the default gateway is always available for the network.

Figure 8 Applications: Device HA


Internet
master
backup

3

Web Configurator

The ZyWALL web configurator allows easy ZyWALL setup and management using an Internet browser.

3.1 Web Configurator Requirements

In order to use the web configurator, you must

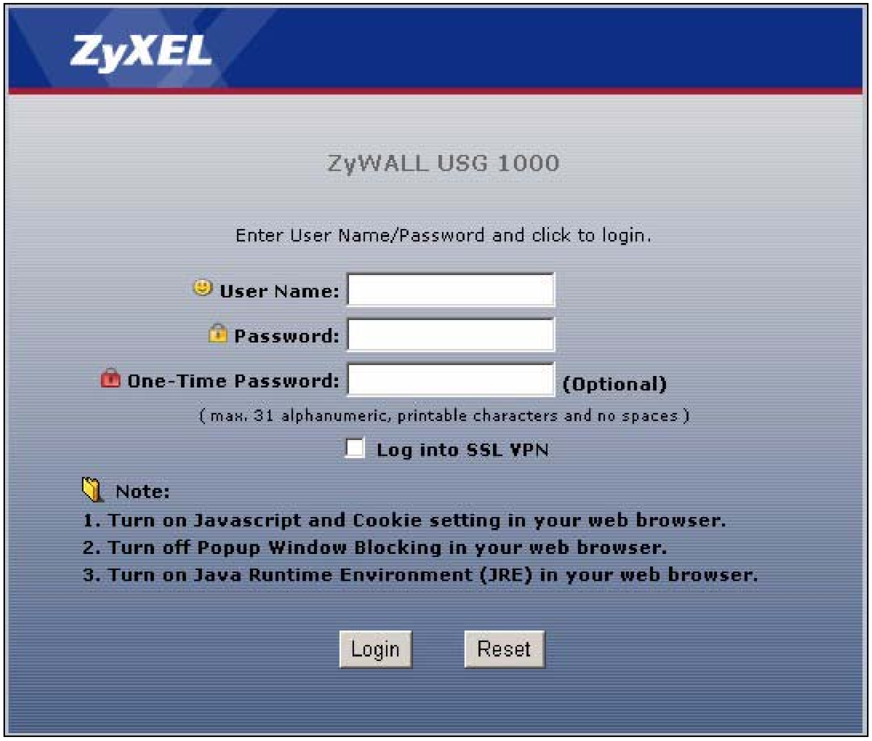
- Use Internet Explorer 6.0 or later, Netscape Navigator 7.2 or later, or Firefox 1.0.7 or later
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

The recommended screen resolution is 1024 x 768 pixels.

3.2 Web Configurator Access

1. Make sure your ZyWALL hardware is properly connected. See the Quick Start Guide.
2. Open your web browser, and go to http://192.168.1.1. By default, the ZyWALL automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears.

Figure 9 Login Screen



ZyWALL USG 1000

Enter User Name/Password and click to login.

User Name:

Password:

One-Time Password: (Optional)

(max. 31 alphanumeric, printable characters and no spaces)

☐ Log into SSL VPN

Note:

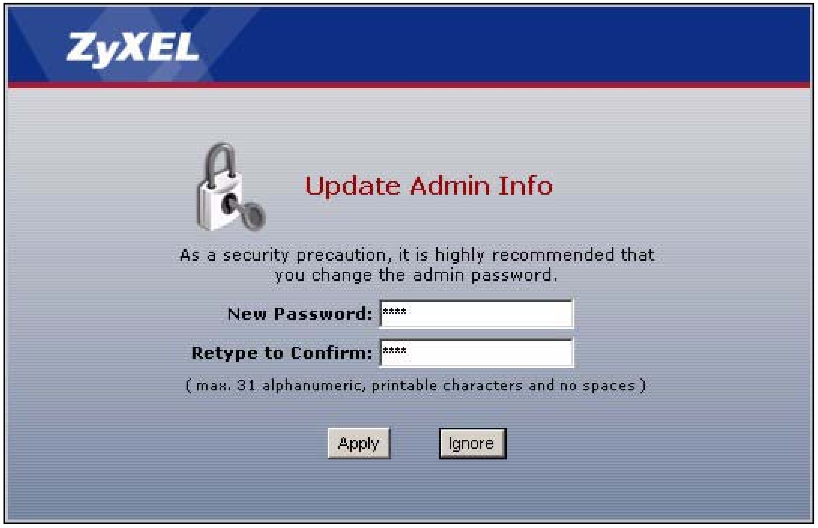
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

3 Type the user name (default: “admin”) and password (default: “1234”).

If your account is configured to use an ASAS authentication server, use the OTP (One-Time Password) token to generate a number. Enter it in the **One-Time Password** field. The number is only good for one login. You must use the token to generate a new number the next time you log in.

4 Click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen (Figure 10 on page 66) appears. Otherwise, the main screen (Figure 11 on page 67) appears.

Figure 10 Update Admin Info Screen



Update Admin Info

As a security precaution, it is highly recommended that you change the admin password.

New Password: ****

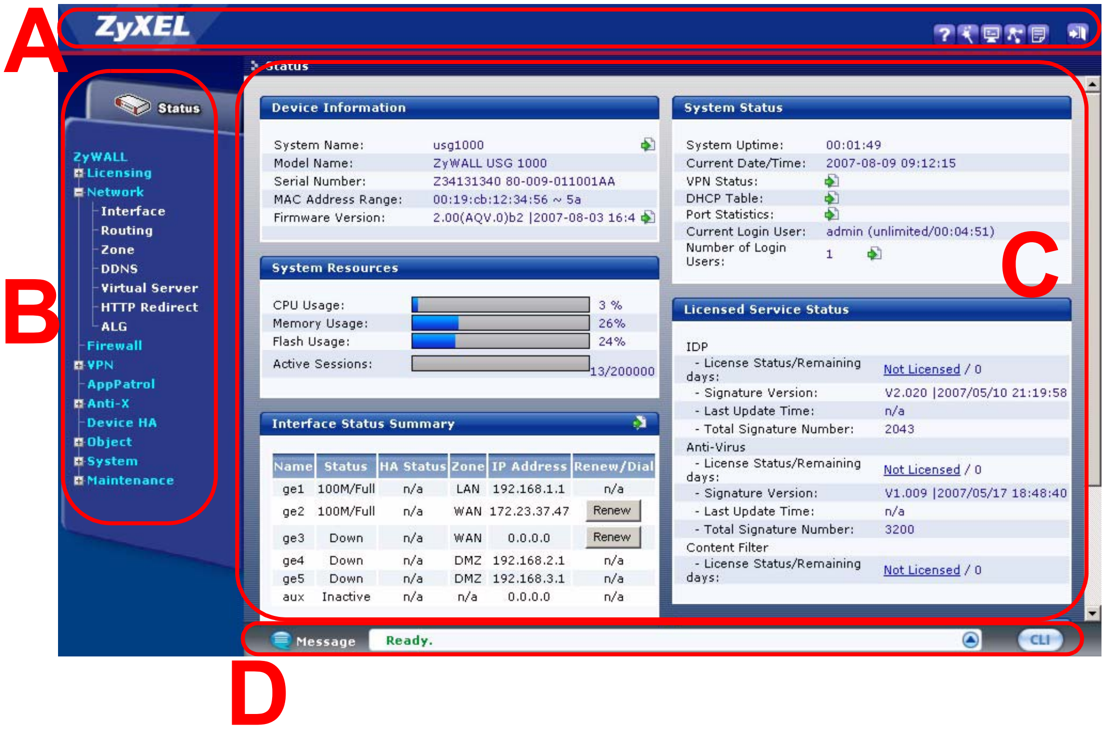
Retype to Confirm: ****

(max. 31 alphanumeric, printable characters and no spaces)

5 The screen above appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

Follow the directions in this screen. If you change the default password, the **Login** screen (Figure 9 on page 66) appears after you click **Apply**. If you click **Ignore**, the main screen appears.

Figure 11 Main Screen



Device Information

System Name: usg1000
Model Name: ZyWALL USG 1000
Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:19:cb:12:34:56 ~ 5a
Firmware Version: 2.00(AQV.0)b2 |2007-08-03 16:4

System Resources

CPU Usage: 3 %
Memory Usage: 26%
Flash Usage: 24%
Active Sessions: 13/200000

Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	100M/Full	n/a	LAN	192.168.1.1	n/a
ge2	100M/Full	n/a	WAN	172.23.37.47	Renew
ge3	Down	n/a	WAN	0.0.0.0	Renew
ge4	Down	n/a	DMZ	192.168.2.1	n/a
ge5	Down	n/a	DMZ	192.168.3.1	n/a
aux	Inactive	n/a	n/a	0.0.0.0	n/a

System Status

System Uptime: 00:01:49
Current Date/Time: 2007-08-09 09:12:15
VPN Status:
DHCP Table:
Port Statistics:
Current Login User: admin (unlimited/00:04:51)
Number of Login Users: 1

Licensed Service Status

IDP
- License Status/Remaining days: Not Licensed / 0
- Signature Version: V2.020 |2007/05/10 21:19:58
- Last Update Time: n/a
- Total Signature Number: 2043

Anti-Virus
- License Status/Remaining days: Not Licensed / 0
- Signature Version: V1.009 |2007/05/17 18:48:40
- Last Update Time: n/a
- Total Signature Number: 3200

Content Filter
- License Status/Remaining days: Not Licensed / 0

Message Ready.

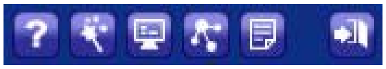
3.3 Web Configurator Main Screen

As illustrated in Figure 11 on page 67, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

3.3.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

Table 5 Title Bar: Web Configurator Icons

ICON	DESCRIPTION
?	**Help**: Click this icon to open the help page for the current screen.
	Wizards: Click this icon to open one of the web configurator wizards. See Chapter 4 on page 75 for more information.
	Console: Click this icon to open the console in which you can use the command line interface (CLI).
	Site Map: Click this icon to display the site map for the web configurator. You can use the site map to go directly to any menu item or any tab in the web configurator.
	About: Click this icon to display basic information about the ZyWALL.
	Logout: Click this icon to log out of the web configurator.

3.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyWALL features. The following tables describe each menu item.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		Use this screen to look at the ZyWALL’s general device information, system status, system resource usage, licensed service status, and interface status.
Licensing		
Registration	Registration	Use this screen to register the device and activate trial services.
	Service	Use this screen to look at the licensed service status and to upgrade licensed services.
Update	IDP/AppPatrol	Use this screen to schedule IDP signature updates and to update signature information immediately.
	System Protect	Use this screen to schedule ADP signature updates and to update signature information immediately.
	Anti-Virus	Use this screen to schedule anti-virus signature updates and to update signature information immediately.
Network		
Interface	Interface Summary	Use this screen to see information about all of the ZyWALL’s interfaces and their connection status.
	Ethernet	Use this screen to manage Ethernet interfaces and virtual Ethernet interfaces.
	Port Grouping	Use this screen to configure physical port groups.
	VLAN	Use this screen to create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Use this screen to create and manage bridges and virtual bridge interfaces.
	PPPoE/PPTP	Use this screen to create and manage PPPoE/PPTP interfaces.
	Auxiliary	Use this screen to manage the **AUX** port.
	Trunk	Use this screen to create and manage trunks for load balancing and link HA.

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Routing	Policy Route	Use this screen to create and manage routing policies.
	Static Route	Use this screen to create and manage IP static routing information.
	RIP	Use this screen to configure device-level RIP settings.
	OSPF	Use this screen to configure device-level OSPF settings, including areas and virtual links.
Zone		Use this screen to configure zones used to define various policies.
DDNS		Use this screen to define and manage domain names and DDNS servers.
Virtual Server		Use this screen to set up and manage port forwarding rules.
HTTP Redirect		Use this screen to set up and manage HTTP redirection rules.
ALG		Use this screen to configure SIP, H.323, and FTP pass-through settings.
Firewall		Use this screen to create and manage level-3 traffic rules.
VPN	VPN Connection	Use this screen to configure IPSec tunnels.
IPSec VPN	VPN Connection	Use this screen to configure IPSec tunnels.
	VPN Gateway	Use this screen to configure IKE tunnels.
	Concentrator	Use this screen to configure VPN concentrators (hub-and-spoke VPN).
	SA Monitor	Use this screen to monitor current IPSec VPN tunnels.
SSL VPN	Access Privilege	Use this screen to configure SSL VPN access rights for users and groups.
	Connection Monitor	Use this screen to monitor current SSL VPN connection.
	Global Setting	Use this screen to configure the ZyWALL's SSL VPN settings that apply to all connections.
L2TP VPN	L2TP Over IPSec	Use this screen to configure L2TP Over IPSec VPN settings.
	Session Monitor	Use this screen to monitor current L2TP Over IPSec VPN sessions.
AppPatrol	General	Use this screen to enable or disable traffic management by application and see registration and signature information.
	Common	Use this screen to manage traffic of the most commonly used web, file transfer and e-mail protocols.
	Instant Messenger	Use this screen to manage instant messenger traffic.
	Peer to Peer	Use this screen to manage peer-to-peer traffic.
	VoIP	Use this screen to manage VoIP traffic.
	Streaming	Use this screen to manage streaming traffic.
	Other	Use this screen to manage other kinds of traffic.
	Statistics	Use this screen to view bandwidth usage and traffic statistics for the protocols that the ZyWALL is managing.
Anti-X		
Anti-Virus	Summary	Use this screen to activate AV scanning on the interface(s), specify actions when a virus is detected, and view registration and signature information.
	Setting	Use this screen to configure AV settings like the white and black lists.
	Signature	Use these screens to search for signatures by signature name or attributes and configure how the ZyWALL uses them.

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
IDP	General	Use this screen to look at and manage IDP bindings.
	Profile	Use this screen to create and manage IDP profiles.
	Custom Signatures	Use this screen to create, import, or export custom signatures.
ADP	General	Use this screen to look at and manage ADP bindings.
	Profile	Use this screen to create and manage ADP profiles.
Content Filter	General	Use this screen to create and manage content filter policies.
	Filtering Profile	Use this screen to create and manage the detailed filtering rules for content filtering policies.
	Cache	Use this screen to manage the URL cache in the ZyWALL.
Device HA	VRRP Group	Use this screen to define and configure virtual groups of redundant routers.
	Synchronize	Use this screen to manage synchronization of ZyWALL configuration between master routers and backup routers in virtual groups of redundant routers.
Object		
User/Group	User	Use this screen to create and manage users.
	Group	Use this screen to create and manage groups of users.
	Setting	Use this screen to manage default settings for all users, general settings for user sessions, and rules to force user authentication.
Address	Address	Use this screen to create and manage host, range, and network (subnet) addresses.
	Address Group	Use this screen to create and manage groups of addresses.
Service	Service	Use this screen to create and manage TCP and UDP services.
	Service Group	Use this screen to create and manage groups of services.
Schedule		Use this screen to create one-time and recurring schedules.
AAA Server	Active Directory-Default	Use this screen to configure the default Active Directory settings.
	Active Directory-Group	Use this screen to create and manage groups of Active Directory servers.
	LDAP-Default	Use this screen to configure the default LDAP settings.
	LDAP-Group	Use this screen to create and manage groups of LDAP servers.
	RADIUS-Default	Use this screen to configure the default RADIUS settings.
	RADIUS-Group	Use this screen to create and manage groups of RADIUS servers.
Auth. Method		Use this screen to create and manage ways of authenticating users.
Certificate	My Certificates	Use this screen to create and manage the ZyWALL's certificates.
	Trusted Certificates	Use this screen to import and manage certificates from trusted sources.
ISP Account		Use this screen to create and manage ISP account information for PPPoE/PPTP interfaces.
SSL Application		Use this screen to create SSL web application or file sharing objects.
System		

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Host Name		Use this screen to configure the system and domain name for the ZyWALL.
Date/Time		Use this screen to configure the current date, time, and time zone in the ZyWALL.
Console Speed		Use this screen to set the console speed.
DNS		Use this screen to configure the DNS server and address records for the ZyWALL.
WWW		Use this screen to configure HTTP, HTTPS, and general authentication.
SSH		Use this screen to configure the SSH server and SSH service settings for the ZyWALL.
TELNET		Use this screen to configure the telnet server settings for the ZyWALL.
FTP		Use this screen to configure the FTP server settings for the ZyWALL.
SNMP		Use this screen to configure SNMP communities and services.
Dial-in Mgmt.		Use this screen to configure settings for an out of band management connection through a modem connected to the **AUX** port.
Vantage CNM		Use this screen to configure and allow your ZyWALL to be managed by the Vantage CNM server.
Language		Use this screen to select the language of the ZyWALL's web configurator screens.
Maintenance		
File Manager	Configuration File	Use this screen to manage and upload configuration files for the ZyWALL.
	Firmware Package	Use this screen to look at the current firmware version and to upload firmware.
	Shell Script	Use this screen to manage and run shell script files for the ZyWALL.
Log	View Log	Use this screen to look at log entries.
	Log Setting	Use this screen to configure the system log, e-mail logs, and remote syslog servers.
Report	Traffic	Use this screen to collect traffic information and display basic reports about it.
	Session	Use this screen to display the status of all current sessions.
	Anti-Virus	Use this screen to collect and display statistics on the viruses that the ZyWALL has detected.
	IDP	Use this screen to collect and display statistics on the intrusions that the ZyWALL has detected.
Diagnostics		Use this screen to have the ZyWALL collect diagnostic information.
Reboot		Use this screen to restart the ZyWALL.

3.3.3 Main Window

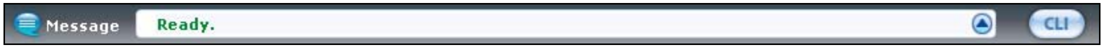
The main window shows the screen you select in the menu. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 7 on page 157 for more information about the **Status** screen.

3.3.4 Message Bar

Check the message bar when you click **Apply** or **OK** to verify that the configuration has been updated.

Figure 12 Message Bar

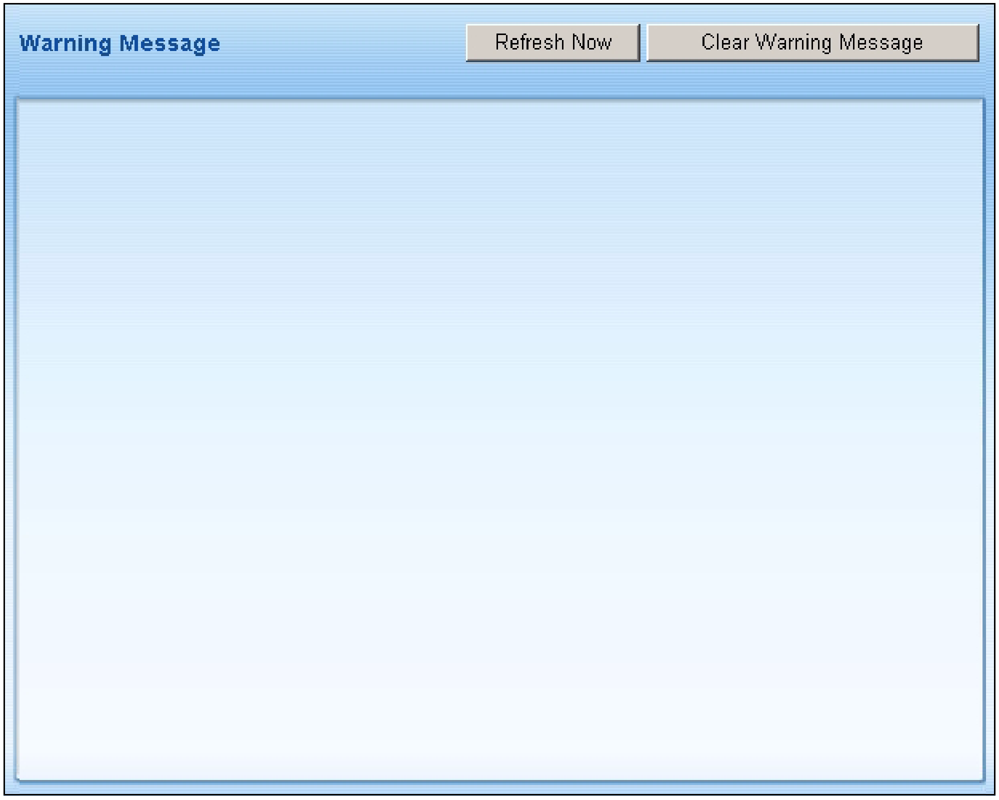


Ready.

3.3.4.1 Warning Messages

Click the up arrow to view the ZyWALL's current warning messages. These warning messages display in a popup window, such as the following.

Figure 13 Warning Messages



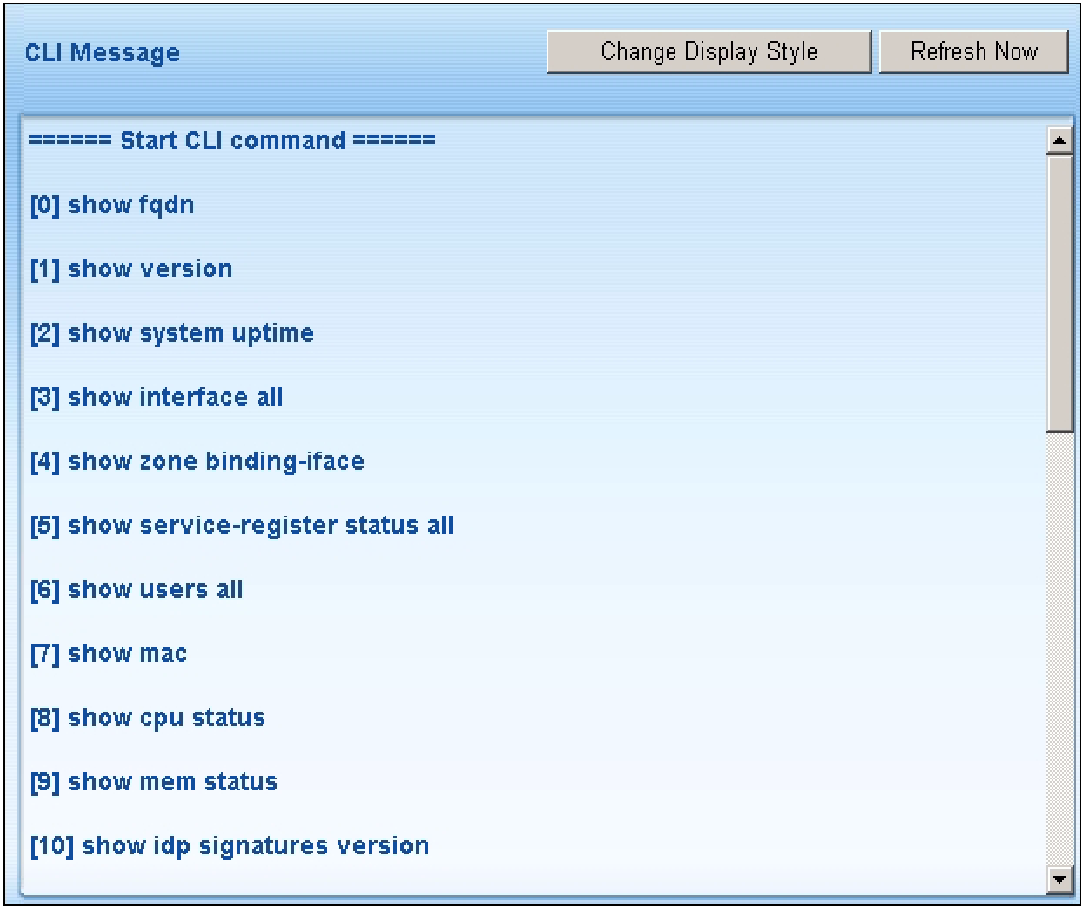
Click **Refresh Now** to update the screen. Close the popup window when you are done with it.

Click **Clear Warning Message** to remove the current warning messages from the window.

3.3.4.2 CLI Messages

Click **CLI** to look at the CLI commands sent by the web configurator. These commands appear in a popup window, such as the following.

Figure 14 CLI Messages



```
====== Start CLI command ======
[0] show fqdn
[1] show version
[2] show system uptime
[3] show interface all
[4] show zone binding-iface
[5] show service-register status all
[6] show users all
[7] show mac
[8] show cpu status
[9] show mem status
[10] show idp signatures version
```

Click **Change Display Style** to show or hide the index numbers for the commands (the commands are more convenient to copy and paste without the index numbers).

Click **Refresh Now** to update the screen. For example, if you just enabled a particular feature, you can look at the commands the web configurator generated to enable it. Close the popup window when you are done with it.

See the Command Reference Guide for information about the commands.

4

Wizard Setup

This chapter provides information on configuring the Wizard setup screens in the web configurator. See the feature-specific chapters in this User's Guide for background information.

4.1 Wizard Setup Overview

Use the wizards only for initial configuration starting from the default configuration.

The web configurator's setup wizards help you configure Internet and VPN connection settings.

Changes you make in an installation or VPN wizard may not be applied if you have already changed the ZyWALL's configuration.

In the ZyWALL web configurator, click the **Wizard** icon to open the **Wizard Setup Welcome** screen. The following summarizes the wizards you can select:

- **INSTALLATION SETUP, ONE ISP**

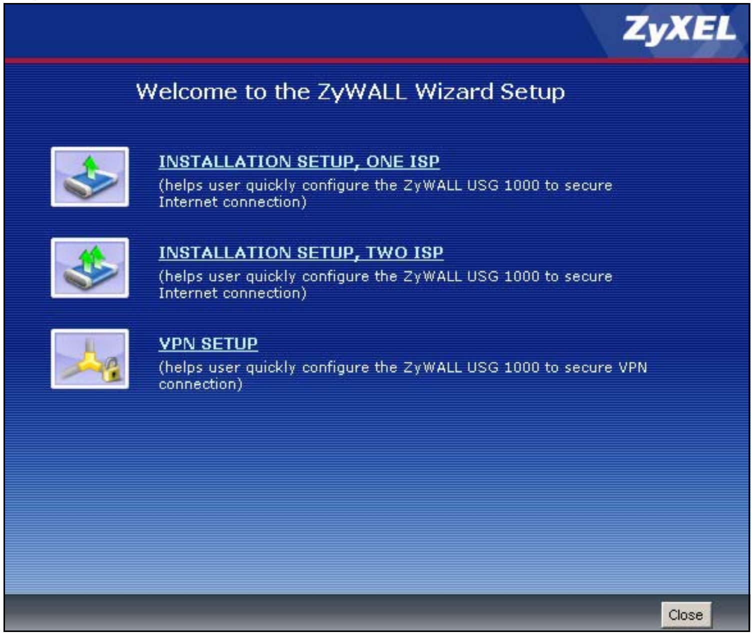
  Click this link to open a wizard to set up a single Internet connection for Gigabit Ethernet port **2**. This wizard creates matching ISP account settings in the ZyWALL if you use PPPoE or PPTP. See Section 4.2 on page 76.
- **INSTALLATION SETUP, TWO ISP**

  Click this link to open a wizard to set up Internet connections for Gigabit Ethernet (ge) interfaces **2** and **3**. See Section 4.5 on page 93. You can connect one interface to one ISP (or network) and connect the other to a second ISP (or network). You can use the second WAN connection for load balancing to increase overall network throughput or as a backup to enhance network reliability (see Section 11.3 on page 219 for more on load balancing).

  This wizard creates matching ISP account settings in the ZyWALL if you use PPPoE or PPTP. This wizard also creates a WAN trunk.
- **VPN SETUP**

Use **VPN SETUP** to configure a VPN connection. See Section 4.6 on page 95.

Figure 15 Wizard Setup Welcome



Welcome to the ZyWALL Wizard Setup

INSTALLATION SETUP, ONE ISP
(helps user quickly configure the ZyWALL USG 1000 to secure Internet connection)

INSTALLATION SETUP, TWO ISP
(helps user quickly configure the ZyWALL USG 1000 to secure Internet connection)

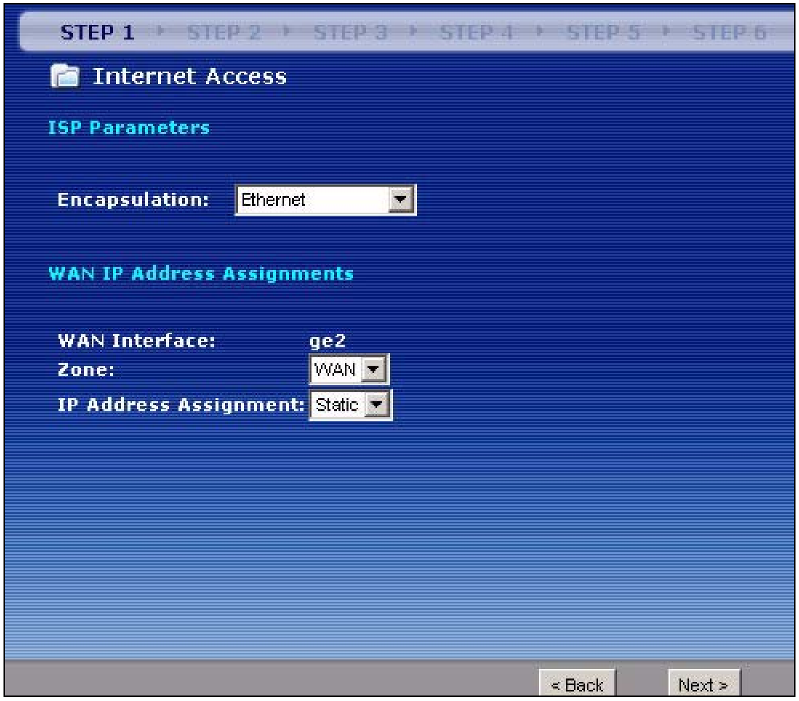
VPN SETUP
(helps user quickly configure the ZyWALL USG 1000 to secure VPN connection)

4.2 Installation Setup, One ISP

The wizard screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Enter the Internet access information exactly as your ISP gave it to you.

Figure 16 Internet Access: Step 1


STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
Internet Access
ISP Parameters
Encapsulation: Ethernet
WAN IP Address Assignments
WAN Interface: ge2
Zone: WAN
IP Address Assignment: Static
< Back
Next >

The following table describes the labels in this screen.

Table 7 Internet Access: Step 1

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.
WAN IP Address Assignments	
WAN Interface	This is the interface you are configuring for Internet access.
Zone	Select the security zone to which you want this interface and Internet connection to belong.
IP Address Assignment	Select **Auto** If your ISP did not assign you a fixed IP address. Select **Static** If the ISP assigned a fixed IP address.
Next	Click **Next** to continue.

4.3 Step 1 Internet Access

Encapsulation: Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.

WAN Interface: This is the interface you are configuring for Internet access.

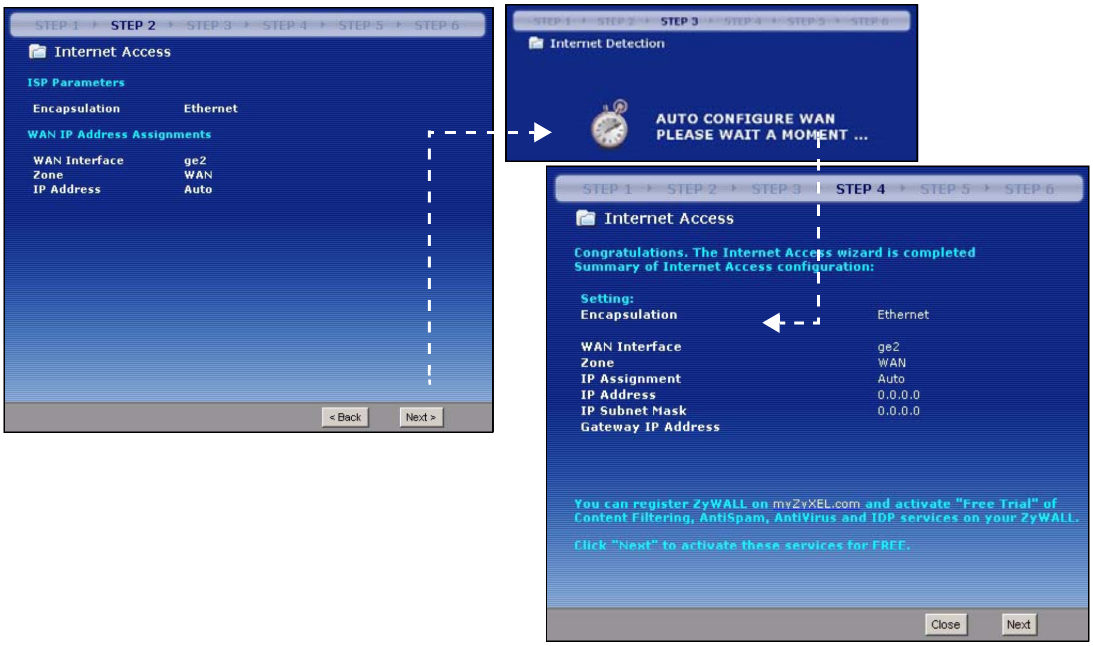
Zone: Select the security zone to which you want this interface and Internet connection to belong.

IP Address Assignment: Select **Auto** If your ISP did not assign you a fixed IP address. Select **Static** If the ISP assigned a fixed IP address.

4.3.1 Ethernet: Auto IP Address Assignment

If you select **Auto** as the **IP Address Assignment** in the previous screen, the following screen displays. Click **Next** to apply the configuration settings.

Figure 17 Ethernet Encapsulation: Auto: Finish



STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 STEP 6
< Back
Next >
STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 STEP 6
STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 STEP 6
Close
Next

Internet Access

ISP Parameters

Encapsulation Ethernet

WAN IP Address Assignments

WAN Interface ge2
Zone WAN
IP Address Auto

Internet Detection

AUTO CONFIGURE WAN
PLEASE WAIT A MOMENT ...

Internet Access

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

Setting:
Encapsulation Ethernet

WAN Interface ge2
Zone WAN
IP Assignment Auto
IP Address 0.0.0.0
IP Subnet Mask 0.0.0.0
Gateway IP Address

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering, AntiSpam, AntiVirus and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

You have set up your ZyWALL to access the Internet.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

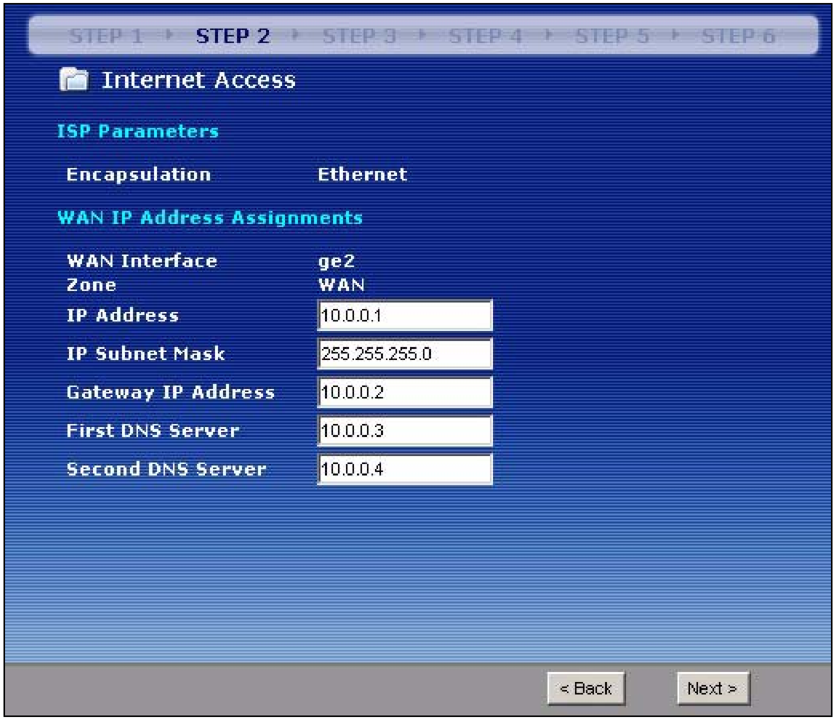
You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.2 Ethernet: Static IP Address Assignment

If you select **Static** as the **IP Address Assignment**, the following screen displays.

Figure 18 Ethernet Encapsulation: Static



ISP Parameters

Encapsulation Ethernet

WAN IP Address Assignments

WAN Interface ge2

Zone WAN

IP Address 10.0.0.1

IP Subnet Mask 255.255.255.0

Gateway IP Address 10.0.0.2

First DNS Server 10.0.0.3

Second DNS Server 10.0.0.4

The following table describes the labels in this screen.

Table 8 Ethernet Encapsulation: Static

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter the IP address that your ISP gave you. This should be a static, public IP address.
IP Subnet Mask	Enter the subnet mask for the IP address.
Gateway IP Address	Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).
First DNS Server Second DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Enter the DNS server IP addresses.
Next	Click **Next** to continue.

The ZyWALL applies the configuration settings.

4.3.3 Step 2 Internet Access Ethernet

You do not configure this screen if you selected **Auto** as the **IP Address Assignment** in the previous screen.

Enter the Internet access information exactly as given to you by your ISP.

WAN Interface: This is the number of the interface that will connect with your ISP.

Zone: This is the security zone to which this interface and Internet connection will belong.

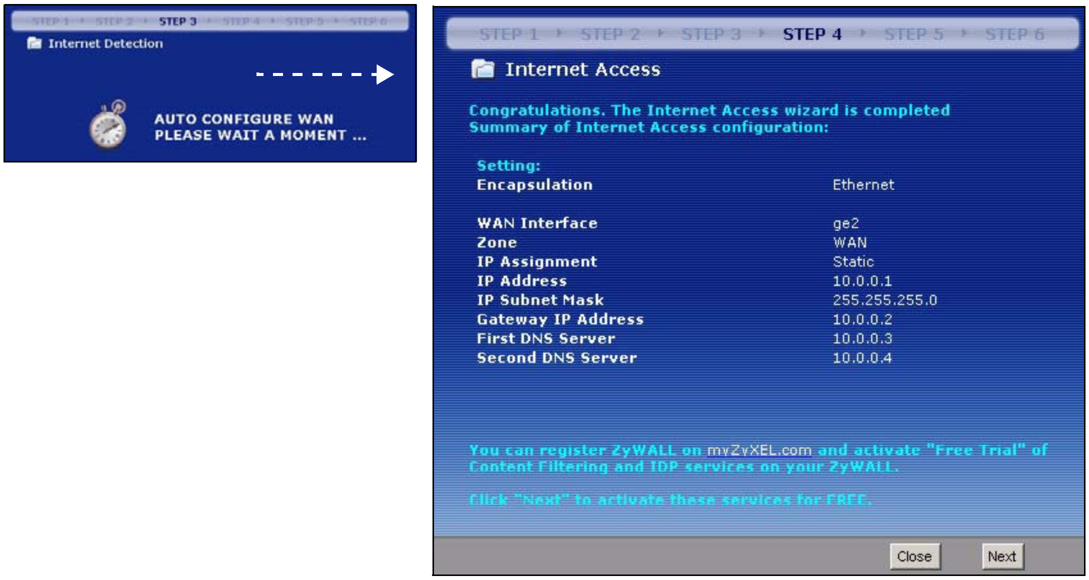
IP Address: Enter your (static) public IP address.

IP Subnet Mask: Enter the subnet mask for this WAN connection's IP address.

Gateway IP Address: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).

DNS Server: The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

Figure 19 Ethernet Encapsulation: Static: Finish



AUTO CONFIGURE WAN
PLEASE WAIT A MOMENT ...

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

Setting:

Encapsulation	Ethernet
WAN Interface	ge2
Zone	WAN
IP Assignment	Static
IP Address	10.0.0.1
IP Subnet Mask	255.255.255.0
Gateway IP Address	10.0.0.2
First DNS Server	10.0.0.3
Second DNS Server	10.0.0.4

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

You have set up your ZyWALL to access the Internet.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

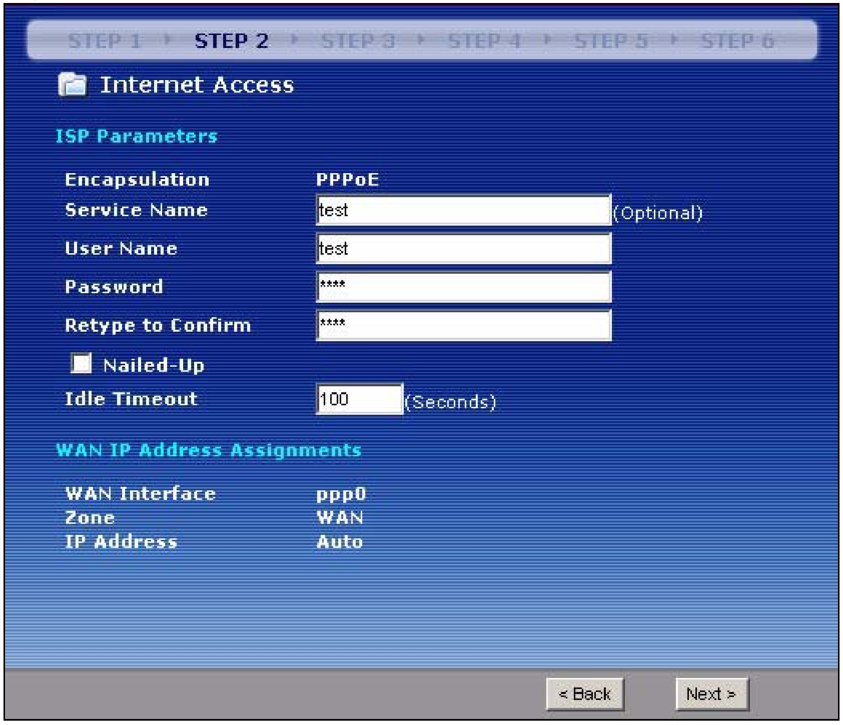
You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.4 PPPoE: Auto IP Address Assignment

If you select **Auto** as the **IP Address Assignment** in the previous screen, the following screen displays after you click **Next**.

Figure 20 PPPoE Encapsulation: Auto



Internet Access

ISP Parameters

Encapsulation PPPoE
Service Name test (Optional)
User Name test
Password ****
Retype to Confirm ****
☐ Nailed-Up
Idle Timeout 100 (Seconds)

WAN IP Address Assignments

WAN Interface ppp0
Zone WAN
IP Address Auto

The following table describes the labels in this screen.

Table 9 PPPoE Encapsulation: Auto

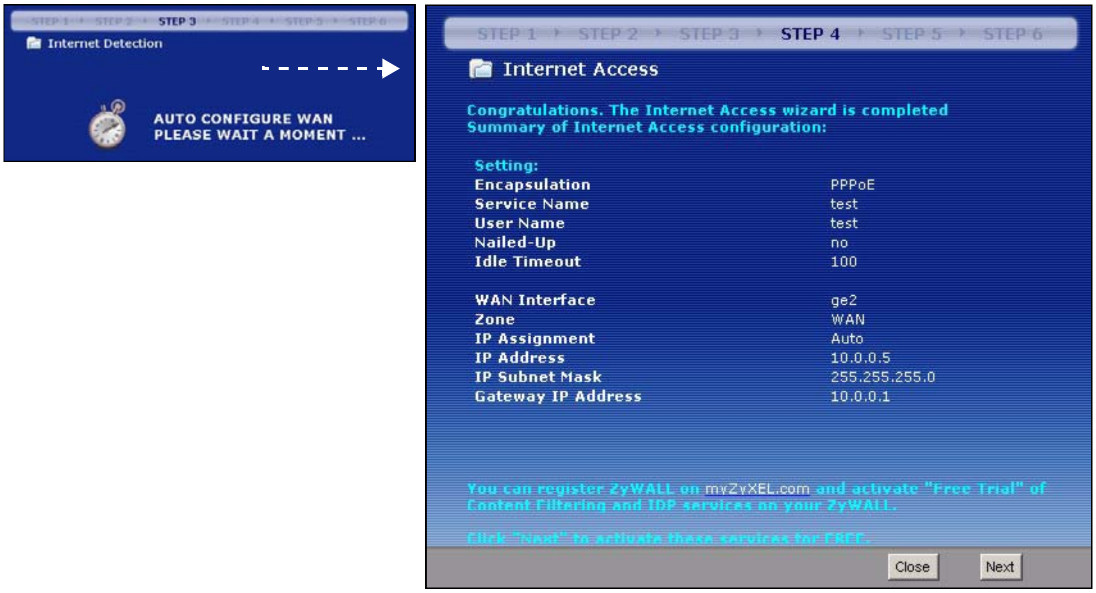
LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
Service Name	Type the PPPoE service name given to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@$./ characters, and it can be up to 64 characters long.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.

Table 9 PPPoE Encapsulation: Auto (continued)

LABEL	DESCRIPTION
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	The ISP will assign your WAN IP address automatically
Next	Click **Next** to continue.

The ZyWALL applies the configuration settings.

Figure 21 PPPoE Encapsulation: Auto: Finish



AUTO CONFIGURE WAN
PLEASE WAIT A MOMENT ...

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

Setting:	
Encapsulation	PPPoE
Service Name	test
User Name	test
Nailed-Up	no
Idle Timeout	100
WAN Interface	ge2
Zone	WAN
IP Assignment	Auto
IP Address	10.0.0.5
IP Subnet Mask	255.255.255.0
Gateway IP Address	10.0.0.1

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

You have set up your ZyWALL to access the Internet.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

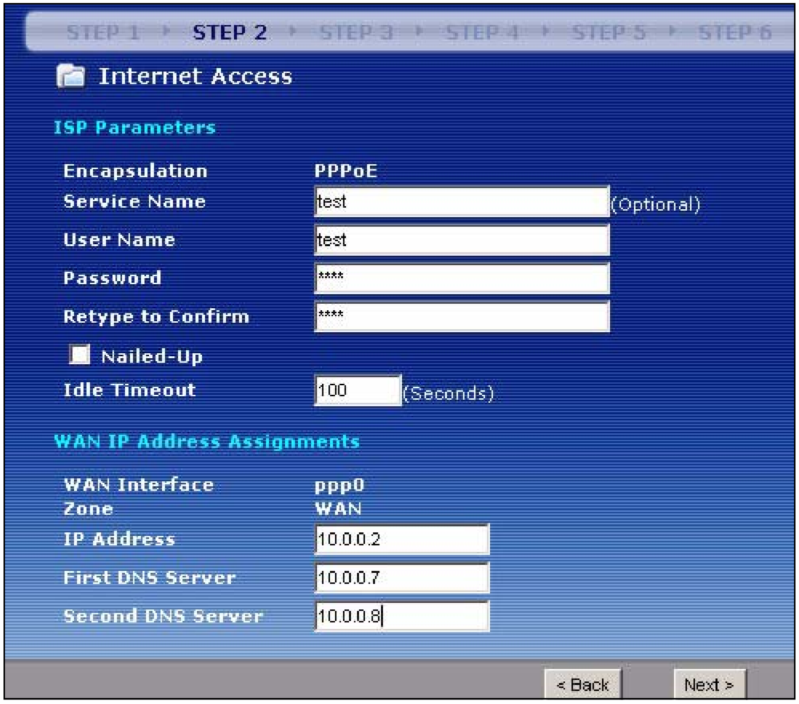
You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.5 PPPoE: Static IP Address Assignment

If you select **Static** as the **IP Address Assignment**, the following screen displays.

Figure 22 PPPoE Encapsulation: Static



Internet Access

ISP Parameters

Encapsulation: PPPoE
Service Name: test (Optional)
User Name: test
Password: ****
Retype to Confirm: ****
☐ Nailed-Up
Idle Timeout: 100 (Seconds)

WAN IP Address Assignments

WAN Interface: ppp0
Zone: WAN
IP Address: 10.0.0.2
First DNS Server: 10.0.0.7
Second DNS Server: 10.0.0.8

The following table describes the labels in this screen.

Table 10 PPPoE Encapsulation: Static

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
Service Name	Type the PPPoE service name given to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@$./ characters, and it can be up to 64 characters long.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter your WAN IP address in this field.
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	

Table 10 PPPoE Encapsulation: Static (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Next	Click **Next** to continue.

4.3.6 Step 2 Internet Access PPPoE

Enter the Internet access information exactly as given to you by your ISP.

4.3.6.1 ISP Parameters

Type the PPPoE **Service Name** from your service provider.

Type the **User Name** given to you by your ISP.

Type the **Password** associated with the user name.

Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPPoE server.

4.3.6.2 WAN IP Address Assignments

You do not configure this section if you selected **Auto** as the **IP Address Assignment** in the previous screen.

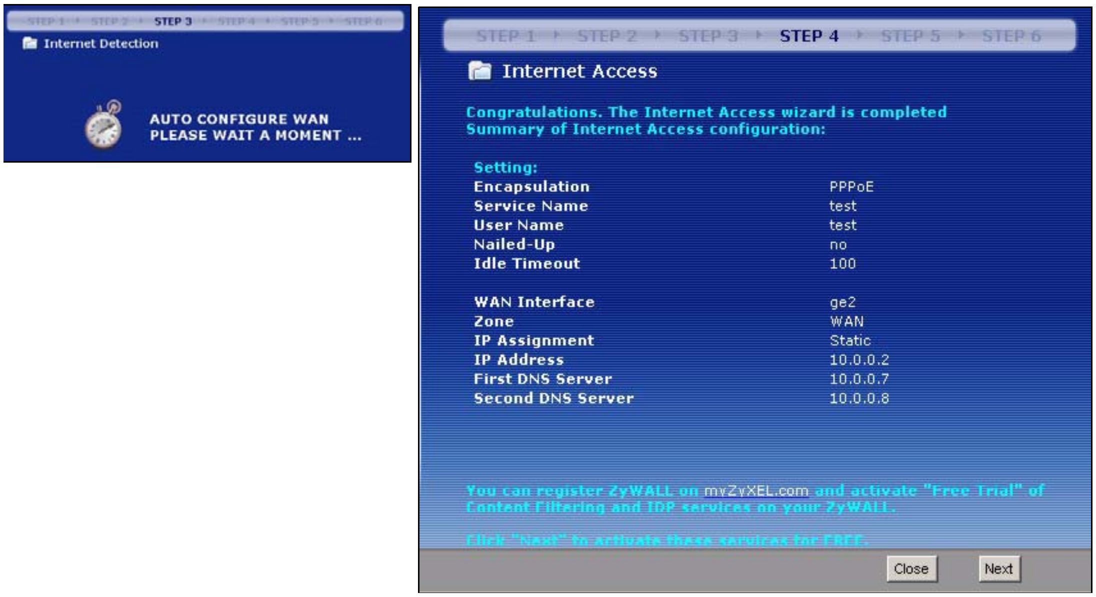
WAN Interface: This is the number of the interface that will connect with your ISP.

Zone: This is the security zone to which this interface and Internet connection will belong.

IP Address: Enter your (static) public IP address.

DNS Server: The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

Figure 23 PPPoE Encapsulation: Static: Finish



AUTO CONFIGURE WAN
PLEASE WAIT A MOMENT ...

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

Setting:

Encapsulation	PPPoE
Service Name	test
User Name	test
Nailed-Up	no
Idle Timeout	100
WAN Interface	ge2
Zone	WAN
IP Assignment	Static
IP Address	10.0.0.2
First DNS Server	10.0.0.7
Second DNS Server	10.0.0.8

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

You have set up your ZyWALL to access the Internet.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

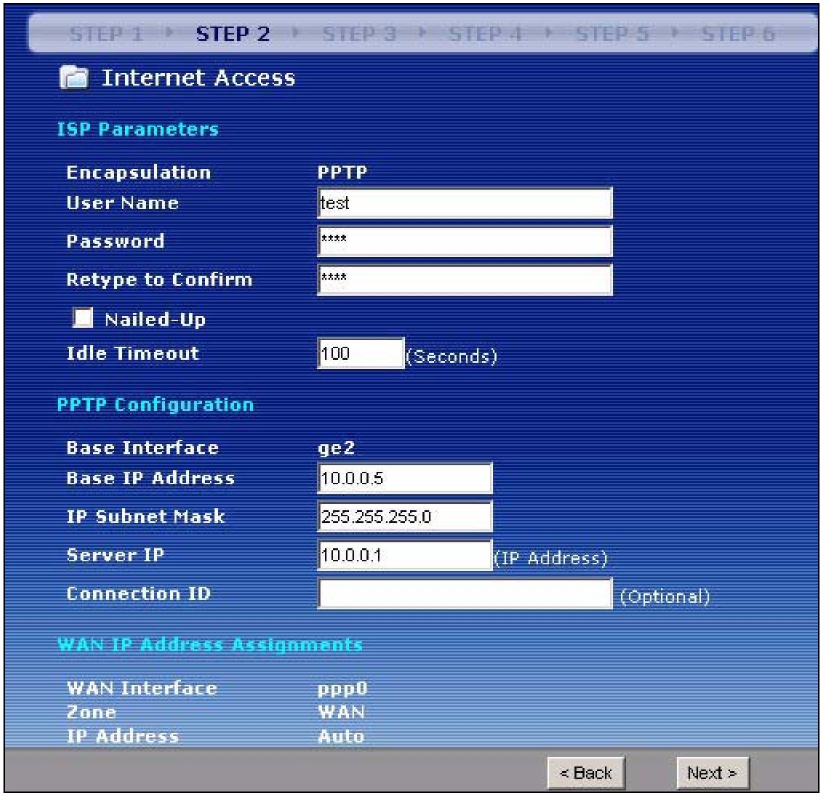
You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.7 PPTP: Auto IP Address Assignment

If you select **Auto** as the **IP Address Assignment** in the previous screen, the following screen displays.

Figure 24 PPTP Encapsulation: Auto



Encapsulation PPTP
User Name test
Password ****
Retype to Confirm ****
☐ Nailed-Up
Idle Timeout 100 (Seconds)

Base Interface ge2
Base IP Address 10.0.0.5
IP Subnet Mask 255.255.255.0
Server IP 10.0.0.1 (IP Address)
Connection ID (Optional)

WAN Interface ppp0
Zone WAN
IP Address Auto

The following table describes the labels in this screen.

Table 11 PPTP Encapsulation: Auto

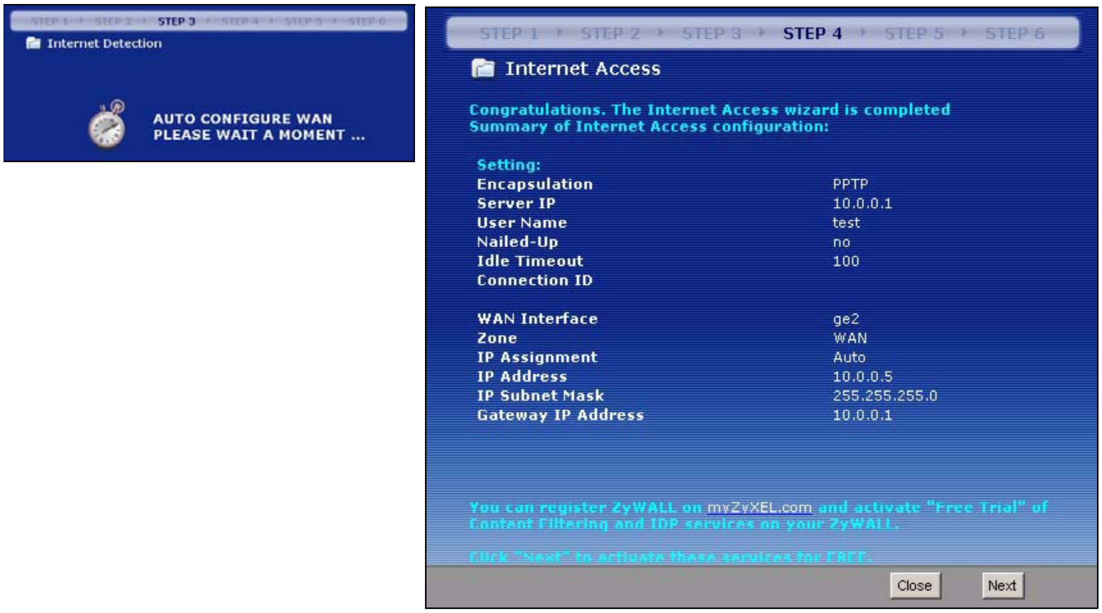
LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP	Type the IP address of the PPTP server.

Table 11 PPTP Encapsulation: Auto (continued)

LABEL	DESCRIPTION
Connection ID	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and `-_:` characters, and it can be up to 31 characters long.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter your WAN IP address in this field.
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Next	Click **Next** to continue.

The ZyWALL applies the configuration settings.

Figure 25 PPTP Encapsulation: Auto: Finish



AUTO CONFIGURE WAN
PLEASE WAIT A MOMENT ...

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

Setting:

Encapsulation	PPTP
Server IP	10.0.0.1
User Name	test
Nailed-Up	no
Idle Timeout	100
Connection ID	
WAN Interface	ge2
Zone	WAN
IP Assignment	Auto
IP Address	10.0.0.5
IP Subnet Mask	255.255.255.0
Gateway IP Address	10.0.0.1

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

You have set up your ZyWALL to access the Internet.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

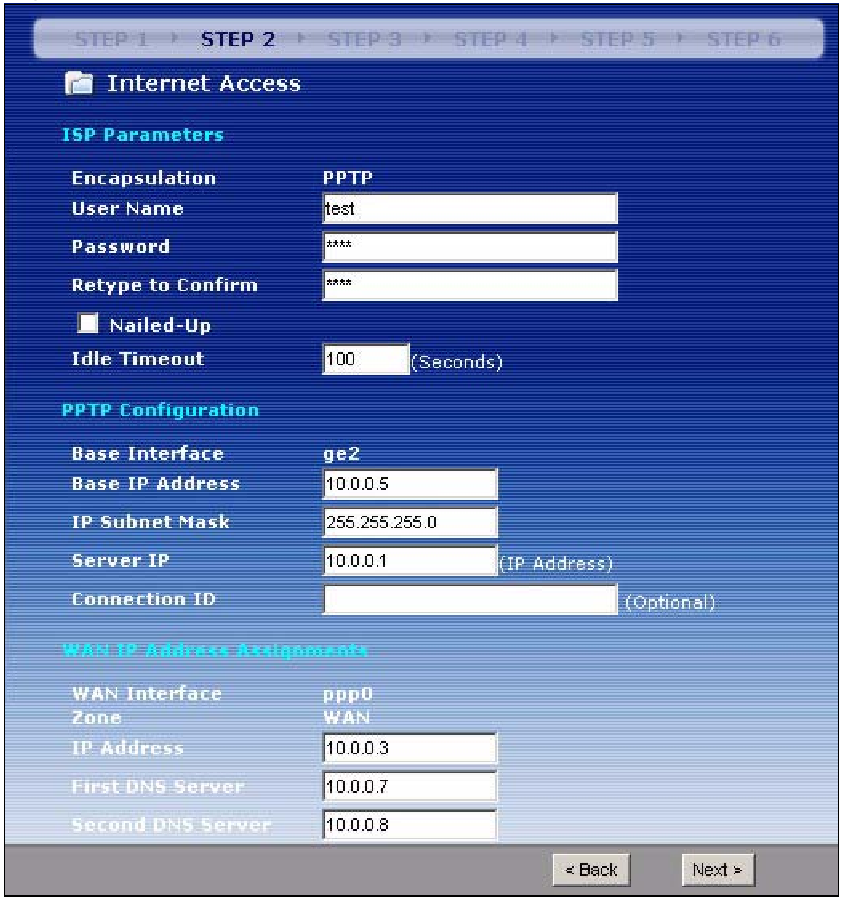
You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.8 PPTP: Static IP Address Assignment

If you select **Static** as the **IP Address Assignment**, the following screen displays.

Figure 26 PPTP Encapsulation: Static



ISP Parameters

Encapsulation PPTP
User Name test
Password ****
Retype to Confirm ****
☐ Nailed-Up
Idle Timeout 100 (Seconds)

PPTP Configuration

Base Interface ge2
Base IP Address 10.0.0.5
IP Subnet Mask 255.255.255.0
Server IP 10.0.0.1 (IP Address)
Connection ID (Optional)

WAN IP Address Assignments

WAN Interface ppp0
Zone WAN
IP Address 10.0.0.3
First DNS Server 10.0.0.7
Second DNS Server 10.0.0.8

The following table describes the labels in this screen.

Table 12 PPTP Encapsulation: Static

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.

Table 12 PPTP Encapsulation: Static (continued)

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -`_@$./` characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP	Type the IP address of the PPTP server.
Connection ID	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and -`_:` characters, and it can be up to 31 characters long. This field can be blank.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter your WAN IP address in this field.
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Next	Click **Next** to continue.

4.3.9 Step 2 Internet Access PPTP

Enter the Internet access information exactly as given to you by your ISP.

4.3.9.1 ISP Parameters

Type the **User Name** given to you by your ISP.

Type the **Password** associated with the user name.

Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPTP server.

4.3.9.2 PPTP Configuration

Base Interface: This is the identity of the Ethernet interface you configure to connect with a modem or router.

Type a **Base IP Address** (static) assigned to you by your ISP.

Type the **IP Subnet Mask** assigned to you by your ISP (if given).

Server IP: Type the IP address of the PPTP server.

Type a **Connection ID** or connection name. It must follow the “c:id” and “n:name” format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your broadband modem or router.

4.3.9.3 WAN IP Address Assignments

You do not configure this section if you selected **Auto** as the **IP Address Assignment** in the previous screen.

WAN Interface: This is the connection type on the interface you are configuring to connect with your ISP.

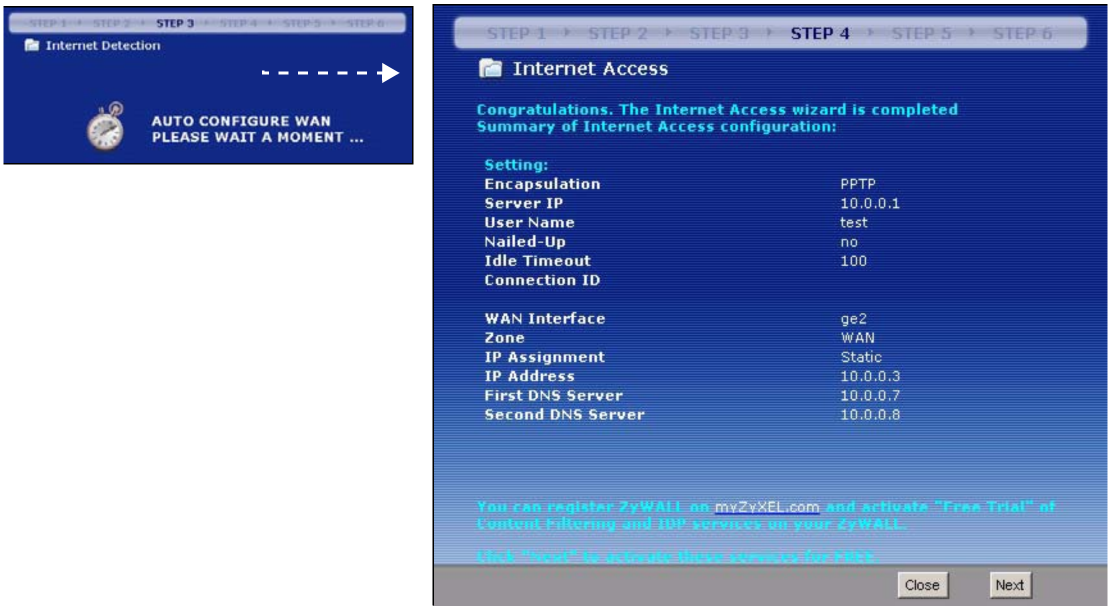
Zone: This is the security zone to which this interface and Internet connection will belong.

IP Address: Enter your (static) public IP address.

DNS Server: The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

The ZyWALL applies the configuration settings.

Figure 27 PPTP Encapsulation: Static: Finish



AUTO CONFIGURE WAN
PLEASE WAIT A MOMENT ...

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

Setting:

Encapsulation	PPTP
Server IP	10.0.0.1
User Name	test
Nailed-Up	no
Idle Timeout	100
Connection ID	
WAN Interface	ge2
Zone	WAN
IP Assignment	Static
IP Address	10.0.0.3
First DNS Server	10.0.0.7
Second DNS Server	10.0.0.8

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

4.3.10 Step 4 Internet Access - Finish

You have set up your ZyWALL to access the Internet.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

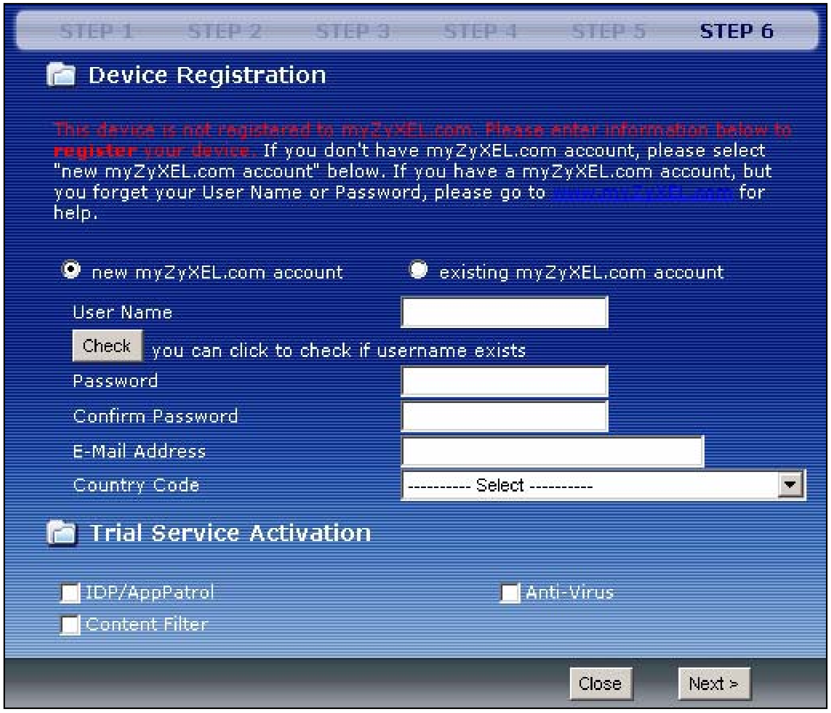
4.4 Device Registration

Use this screen to register your ZyWALL with myZXEL.com and activate trial periods of subscription security features if you have not already done so.

You must be connected to the Internet to register.

This screen displays a read-only user name and password if the ZyWALL is already registered. It also shows which trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Registration > Service** screen to update your service subscription status.

Figure 28 Registration


STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
Device Registration
● new myZyXEL.com account
○ existing myZyXEL.com account
User Name
Check
you can click to check if username exists
Password
Confirm Password
E-Mail Address
Country Code
---------- Select ----------
Trial Service Activation
☐ IDP/AppPatrol
☐ Anti-Virus
☐ Content Filter
Close
Next >

This device is not registered to myZyXEL.com. Please enter information below to **register** your device. If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have a myZyXEL.com account, but you forget your User Name or Password, please go to www.myZyXEL.com for help.

The following table describes the labels in this screen.

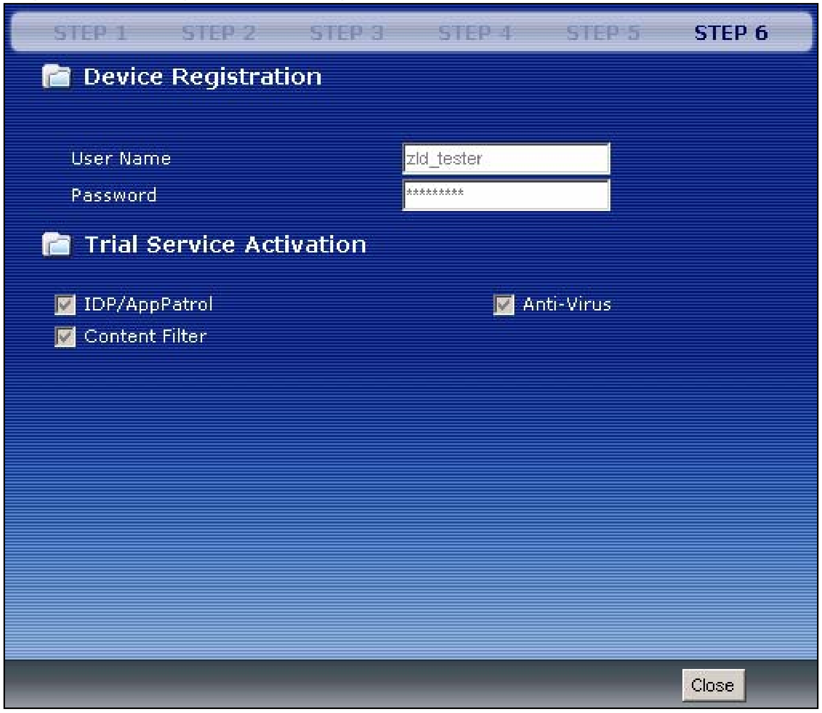
Table 13 Registration

LABEL	DESCRIPTION
Device Registration	If you select **existing myZyXEL.com account**, only the **User Name** and **Password** fields are available.
new myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL.
existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL.
UserName	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country Code	Select your country from the drop-down box list.
Trial Service Activation	You can try a trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the **Registration Service** screen to extend the service.
IDP/AppPatrol Anti-Virus Content Filter	Select the check box to activate a trial. The trial period starts the day you activate the trial.

Table 13 Registration (continued)

LABEL	DESCRIPTION
Close	Click **Close** to exit the wizard.
Next	Click **Next** to save your changes back to the ZyWALL and activate the selected services.

Figure 29 Registration: Registered Device


STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
Device Registration

User Name zld_tester

Password *********

Trial Service Activation

☑ IDP/AppPatrol

☑ Anti-Virus

☑ Content Filter

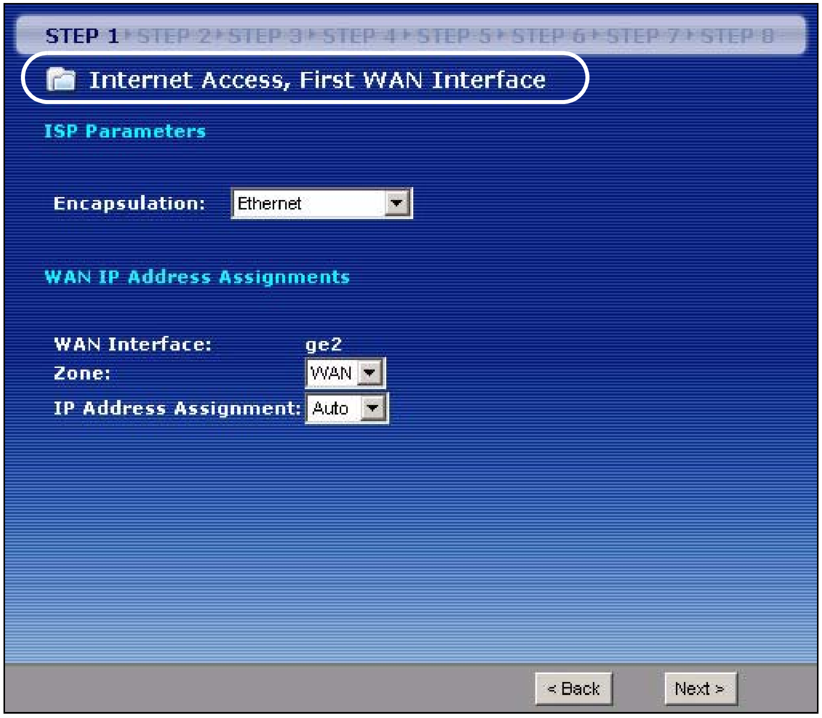
Close

4.5 Installation Setup, Two Internet Service Providers

This wizard allows you to configure two interfaces for Internet access through either two different Internet Service Providers (ISPs) or two different accounts with the same ISP.

The configuration of the following screens is explained in Section 4.2 on page 76 section. Configure the **First WAN Interface** and click **Next**.

Figure 30 Internet Access: Step 1: First WAN Interface



STEP 1 ▸ STEP 2 ▸ STEP 3 ▸ STEP 4 ▸ STEP 5 ▸ STEP 6 ▸ STEP 7 ▸ STEP 8

Internet Access, First WAN Interface

ISP Parameters

Encapsulation: Ethernet

WAN IP Address Assignments

WAN Interface: ge2

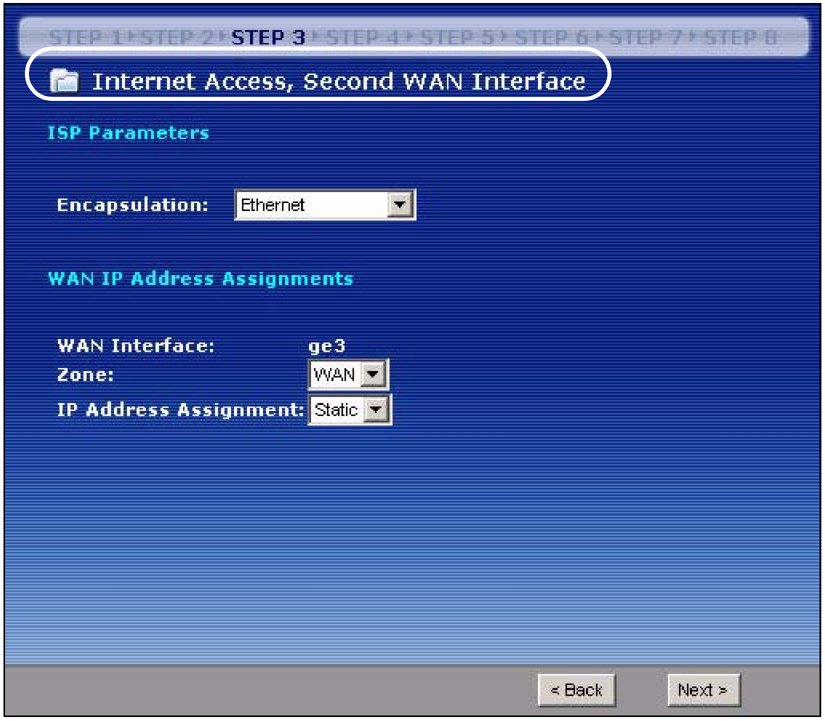
Zone: WAN

IP Address Assignment: Auto

< Back
Next >

After you configure the **First WAN Interface**, you can configure the **Second WAN Interface**. Click **Next** to continue.

Figure 31 Internet Access: Step 3: Second WAN Interface



STEP 1 ▸ STEP 2 ▸ STEP 3 ▸ STEP 4 ▸ STEP 5 ▸ STEP 6 ▸ STEP 7 ▸ STEP 8

Internet Access, Second WAN Interface

ISP Parameters

Encapsulation: Ethernet

WAN IP Address Assignments

WAN Interface: ge3

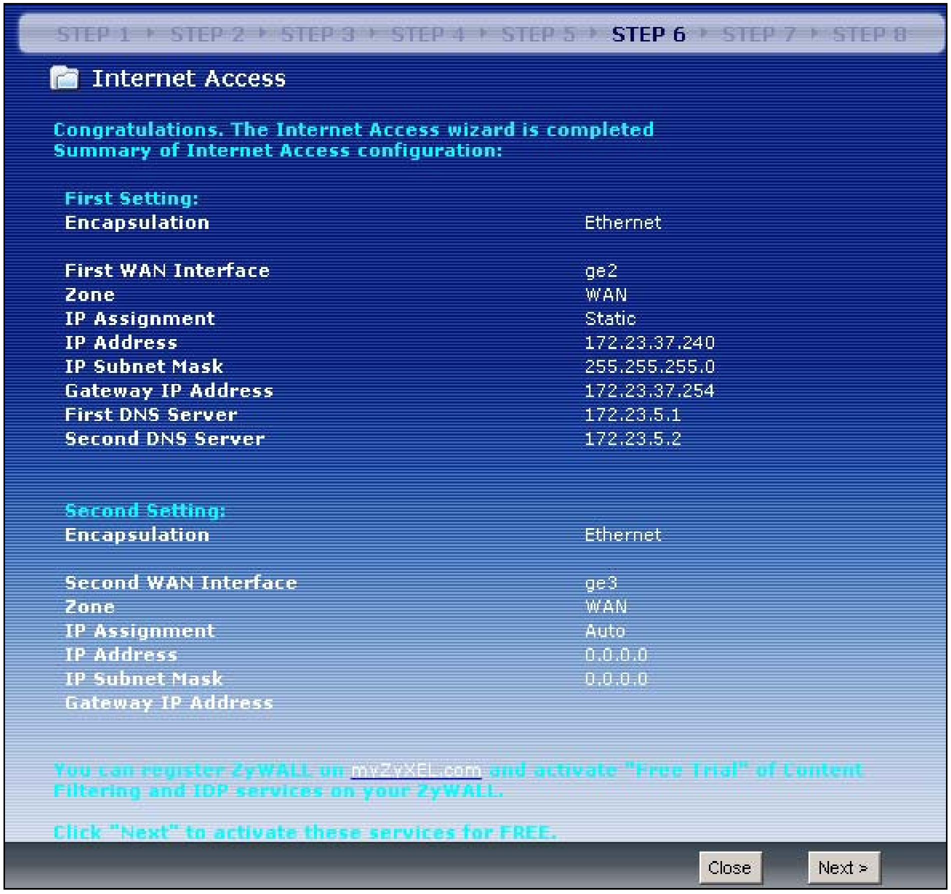
Zone: WAN

IP Address Assignment: Static

< Back
Next >

After you configure the **Second WAN Interface**, a summary of configuration settings display for both WAN interfaces.

Figure 32 Internet Access: Finish



Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

First Setting:

Encapsulation	Ethernet
First WAN Interface	ge2
Zone	WAN
IP Assignment	Static
IP Address	172.23.37.240
IP Subnet Mask	255.255.255.0
Gateway IP Address	172.23.37.254
First DNS Server	172.23.5.1
Second DNS Server	172.23.5.2

Second Setting:

Encapsulation	Ethernet
Second WAN Interface	ge3
Zone	WAN
IP Assignment	Auto
IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filtering and IDP services on your ZyWALL.

Click "Next" to activate these services for FREE.

You can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

Use the myZyXEL.com link if you do already have a myZyXEL.com account. If you already have a myZyXEL.com account, you can click **Next** and use the following screen to register your ZyWALL and activate service trials (see Section 4.4 on page 91).

Alternatively, click **Close** to exit the wizard.

4.5.1 Internet Access Wizard Setup Complete

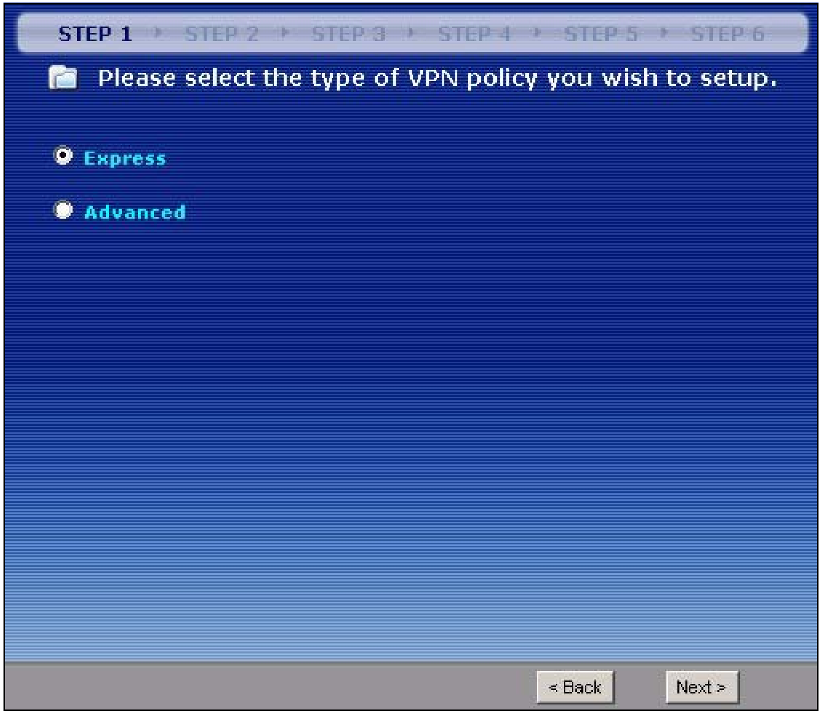
Well done! You have successfully set up your ZyWALL to access the Internet.

4.6 VPN Setup

The VPN wizard creates corresponding VPN connection and VPN gateway settings, a policy route and address objects that you can use later in configuring more VPN connections or other features.

Click **VPN SETUP** in the Wizard Setup Welcome screen (Figure 15 on page 76) to open the following screen. Use it to select which type of VPN settings you want to configure.

Figure 33 VPN Wizard: Wizard Type



Please select the type of VPN policy you wish to setup.

● Express

○ Advanced

The following table describes the labels in this screen.

Table 14 VPN Wizard: Step 1: Wizard Type

LABEL	DESCRIPTION
Express	Use this wizard to create a VPN connection with another ZLD-based ZyWALL using a pre-shared key and default security settings.
Advanced	Use this wizard to configure detailed VPN security settings such as using certificates. The VPN connection can be to another ZLD-based ZyWALL or other IPSec device.
Next	Click **Next** to continue.

4.7 VPN Wizards

A VPN (Virtual Private Network) tunnel is a secure connection to another computer or network.

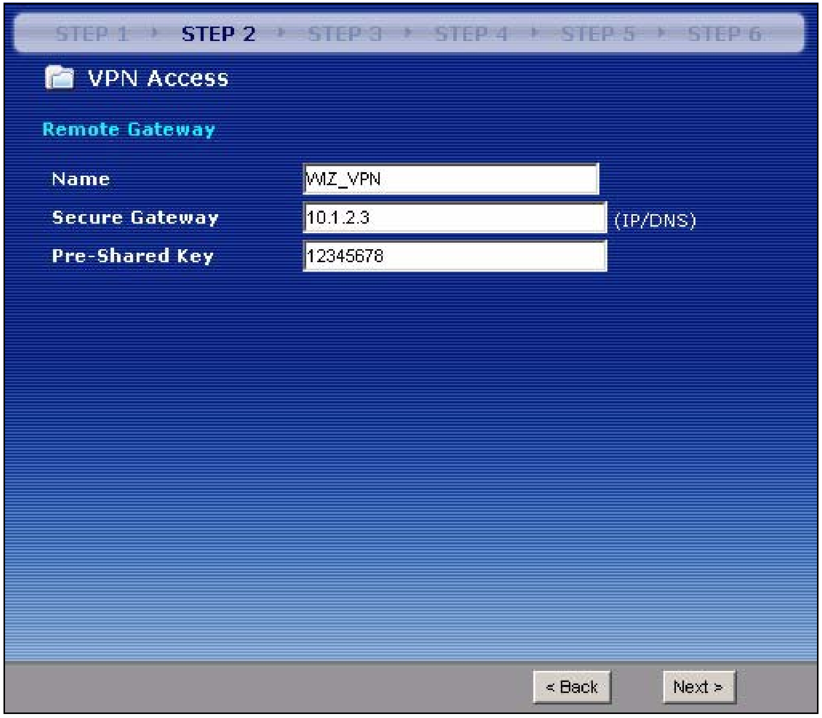
Use the **Express** wizard to create a VPN connection with another ZLD-based ZyWALL using a pre-shared key and default security settings.

Use the **Advanced** wizard to configure detailed VPN security settings such as using certificates. The VPN connection can be to another ZLD-based ZyWALL or other IPSec devices.

4.7.1 VPN Express Wizard

Click the **Express** radio button as shown in Figure 33 on page 96 to display the following screen.

Figure 34 VPN Express Wizard: Step 2



Name: WIZ_VPN
Secure Gateway: 10.1.2.3 (IP/DNS)
Pre-Shared Key: 12345678

The following table describes the labels in this screen.

Table 15 VPN Express Wizard: Step 2

LABEL	DESCRIPTION
Name	Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Secure Gateway	Enter the WAN IP address or domain name of the remote IPSec router (secure gateway) to identify the remote IPSec router by its IP address or a domain name. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. Precede hexadecimal characters with “0x”. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Next	Click **Next** to continue.

4.8 VPN Express Wizard - Remote Gateway

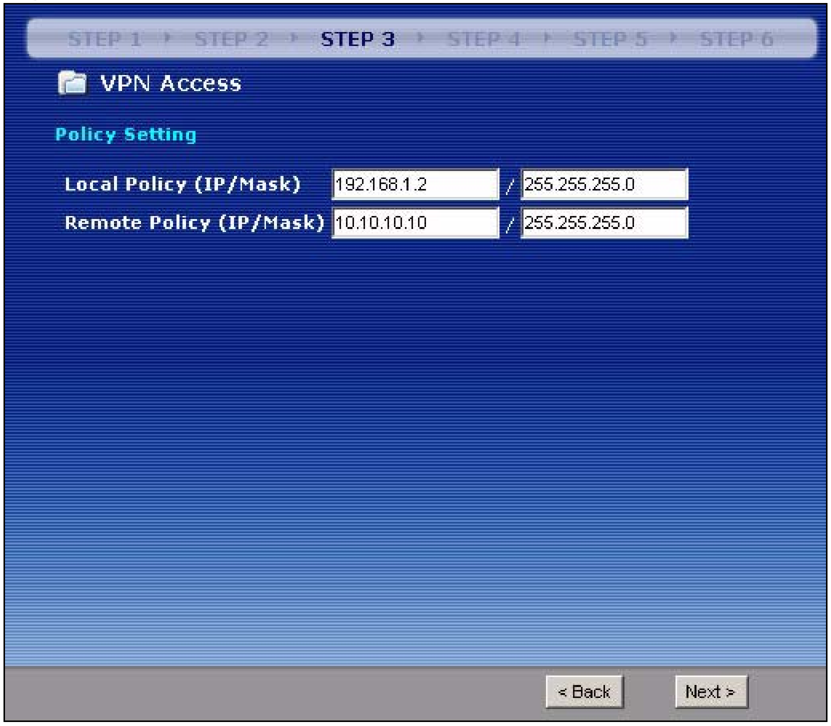
The **Remote Gateway** policy identifies the IPSec devices at either end of a VPN tunnel.

Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Secure Gateway: Enter the WAN IP address or domain name of the remote IPSec router (secure gateway). Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address and no domain name.

Pre-Shared Key: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 16 to 62 hexadecimal (“0-9”, “A-F”) characters. Proceed hexadecimal characters with “0x”.

Figure 35 VPN Express Wizard: Step 3



Local Policy (IP/Mask) 192.168.1.2 / 255.255.255.0

Remote Policy (IP/Mask) 10.10.10.10 / 255.255.255.0

The following table describes the labels in this screen.

Table 16 VPN Express Wizard: Step 3

LABEL	DESCRIPTION
Local Policy (IP/Mask)	Type a static local IP address that corresponds to the remote IPSec router's configured remote IP address (the remote IP address of the other ZyWALL). To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind your ZyWALL.
Remote Policy (IP/Mask)	Type a static local IP address that corresponds to the remote IPSec router's configured local IP address (the local IP address of the other ZyWALL). To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind the remote gateway.
Next	Click **Next** to continue.

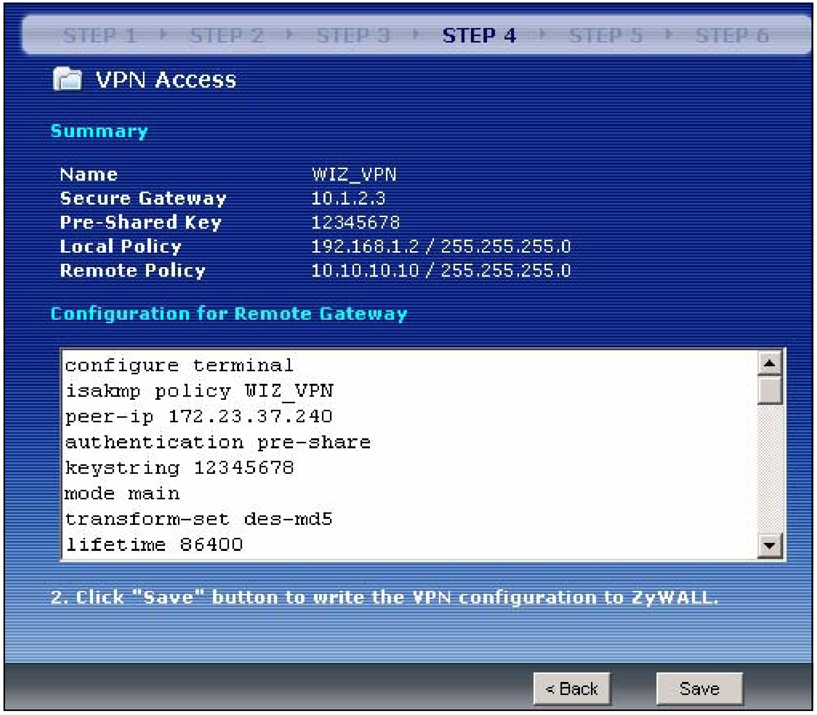
4.8.1 VPN Express Wizard - Policy Setting

The **Policy Setting** specifies which devices can use the VPN tunnel. Local and remote IP addresses must be static.

Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the peer IPSec device.

Remote Policy (IP/Mask): Type the IP address of a computer behind the peer IPSec device. You can also specify a subnet. This must match the local IP address configured on the peer IPSec device.

Figure 36 VPN Express Wizard: Step 4



Summary

Name	WIZ_VPN
Secure Gateway	10.1.2.3
Pre-Shared Key	12345678
Local Policy	192.168.1.2 / 255.255.255.0
Remote Policy	10.10.10.10 / 255.255.255.0

Configuration for Remote Gateway

```
configure terminal
isakmp policy WIZ_VPN
peer-ip 172.23.37.240
authentication pre-share
keystring 12345678
mode main
transform-set des-md5
lifetime 86400
```

2. Click "Save" button to write the VPN configuration to ZyWALL.

The following table describes the labels in this screen.

Table 17 VPN Express Wizard: Step 4

LABEL	DESCRIPTION
Summary	
Name	This is the name of the VPN connection (and VPN gateway).
Secure Gateway	This is the WAN IP address or domain name of the remote IPSec router. If this field displays **0.0.0.0**, only the remote IPSec router can initiate the VPN connection.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
Local Policy	This is a (static) IP address and Subnet Mask on the LAN behind your ZyWALL.
Remote Policy	This is a (static) IP address and Subnet Mask on the network behind the remote IPSec router.

Table 17 VPN Express Wizard: Step 4 (continued)

LABEL	DESCRIPTION
Configuration for Remote Gateway	These commands set the matching VPN connection settings for the remote gateway. If the remote gateway is a ZLD-based ZyWALL, you can copy and paste this list into its command line interface in order to configure it for the VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.
Save	Click **Save** to store the VPN settings on your ZyWALL.

4.8.2 VPN Express Wizard - Summary

This summary of VPN tunnel settings is read-only.

Name: Identifies the VPN gateway policy.

Secure Gateway: IP address or domain name of the peer IPSec device.

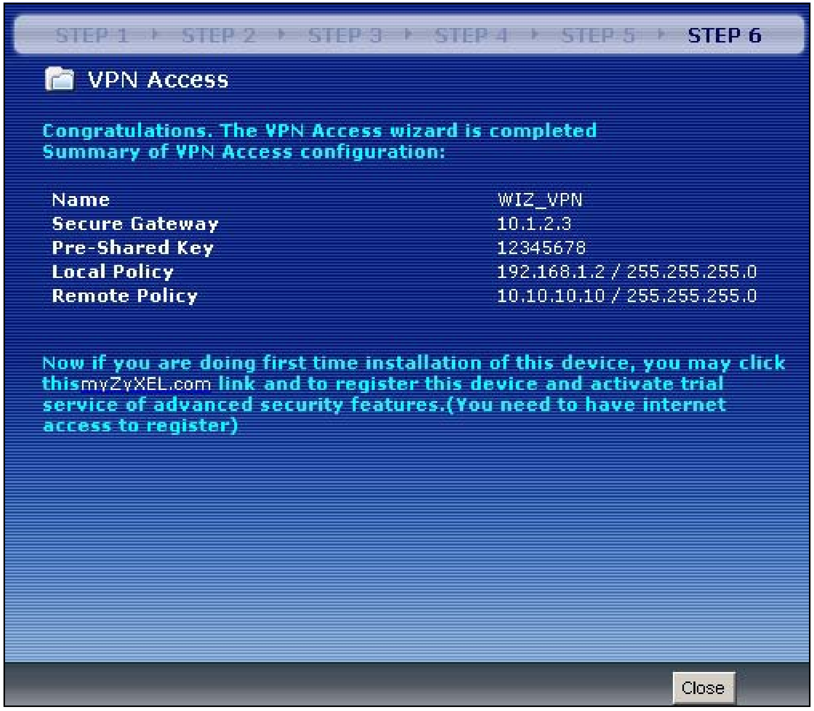
Pre-Shared Key: VPN tunnel password.

Local Policy: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.

Remote Policy: IP address and subnet mask of the computers on the network behind the peer IPSec device that can use the tunnel.

You can copy and paste the **Configuration for Remote Gateway** commands into another ZLD-based ZyWALL's command line interface.

Figure 37 VPN Express Wizard: Step 6



Congratulations. The VPN Access wizard is completed
Summary of VPN Access configuration:

Name	WIZ_VPN
Secure Gateway	10.1.2.3
Pre-Shared Key	12345678
Local Policy	192.168.1.2 / 255.255.255.0
Remote Policy	10.10.10.10 / 255.255.255.0

Now if you are doing first time installation of this device, you may click thismyZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)

If you have not already done so, use the myZyXEL.com link and register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

Alternatively, click **Close** to exit the wizard.

4.8.3 VPN Express Wizard - Finish

Now you can use the VPN tunnel.

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

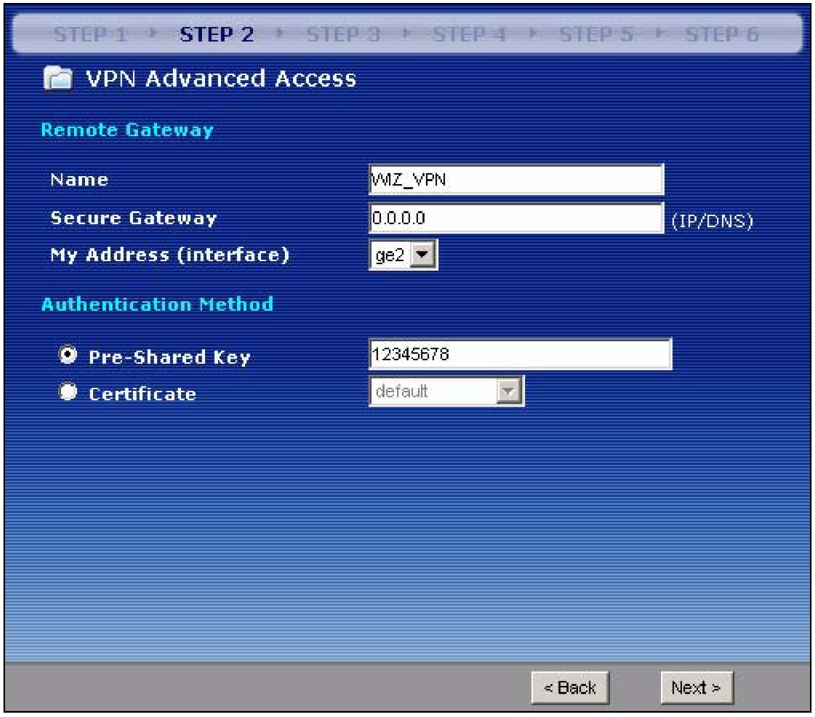
You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.8.4 VPN Advanced Wizard

Click the **Advanced** radio button as shown in Figure 33 on page 96 to display the following screen.

Figure 38 VPN Advanced Wizard: Step 2



Name: WIZ_VPN
Secure Gateway: 0.0.0.0 (IP/DNS)
My Address (interface): ge2
● Pre-Shared Key: 12345678
○ Certificate: default

The following table describes the labels in this screen.

Table 18 VPN Advanced Wizard: Step 2

LABEL	DESCRIPTION
Remote Gateway	
Name	Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Secure Gateway	Enter the WAN IP address or domain name of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by its IP address or a domain name. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.
My Address (interface)	Select an interface from the drop-down list box to use on your ZyWALL.
Authentication Method	
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. Precede hexadecimal characters with “0x”. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.

Table 18 VPN Advanced Wizard: Step 2 (continued)

LABEL	DESCRIPTION
Certificate	Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **Certificate** under the **Object** menu to go to the **My Certificates** screen where you can view the ZyWALL's list of certificates.
Next	Click **Next** to continue.

4.8.5 VPN Advanced Wizard - Remote Gateway

The **Remote Gateway** policy identifies the IPSec devices at either end of a VPN tunnel.

Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Secure Gateway: Enter the WAN IP address or domain name of the remote IPSec router (secure gateway). Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address and no domain name.

Select an interface to use on your ZyWALL.

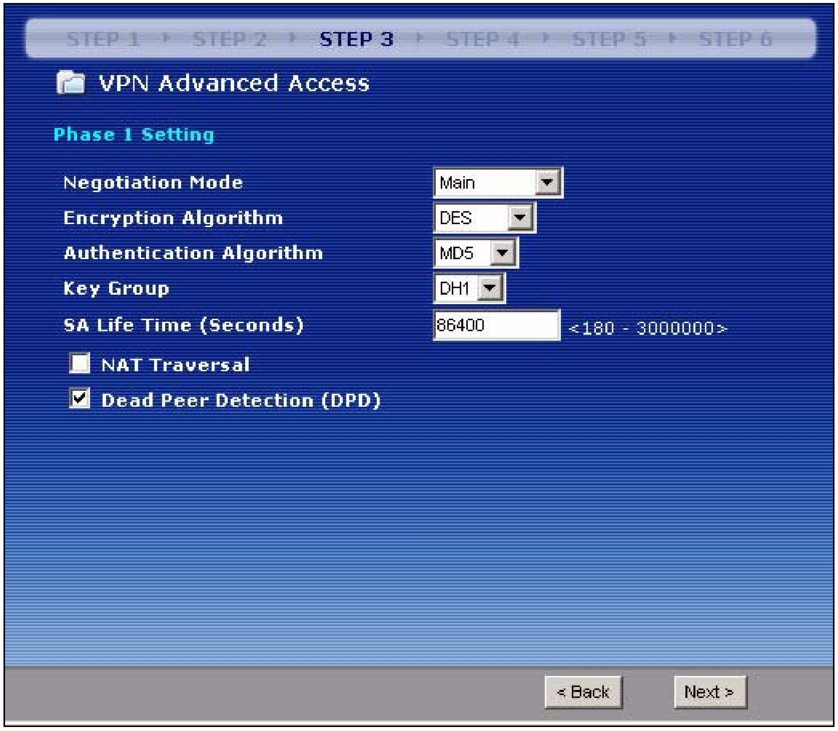
Select **Pre-Shared Key** to use a password for authentication. Both ends of the VPN tunnel must use the same pre-shared key. Use 8 to 31 case-sensitive ASCII characters or 16 to 62 hexadecimal (“0-9”, “A-F”) characters. Precede hexadecimal characters with “0x”.

Select **Certificate** to use a digital certificate for authentication. default uses the ZyWALL's default certificate. Click **Object > Certificate** to configure other certificates in the **My Certificates** screen.

4.8.5.1 Phase 1 Setting

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Figure 39 VPN Advanced Wizard: Step 3



Negotiation Mode: Main
Encryption Algorithm: DES
Authentication Algorithm: MD5
Key Group: DH1
SA Life Time (Seconds): 86400 <180 - 3000000>
☐ NAT Traversal
☑ Dead Peer Detection (DPD)

The following table describes the labels in this screen.

Table 19 VPN Advanced Wizard: Step 3

LABEL	DESCRIPTION
Negotiation Mode	Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords. Note: Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. **AES128** uses a 128-bit key and is faster than **3DES**. **AES192** uses a 192-bit key and **AES256** uses a 256-bit key. Select **Null** to have no encryption.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA1** for maximum security.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536 bit random number.

Table 19 VPN Advanced Wizard: Step 3 (continued)

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 60 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. Note: The remote IPSec router must also have NAT traversal enabled. See Section 20.4.2.2 on page 311 for more information.
Dead Peer Detection (DPD)	Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec server. If the remote IPSec server responds, the ZyWALL transmits the data. If the remote IPSec server does not respond, the ZyWALL shuts down the IKE SA.
Next	Click **Next** to continue.

4.8.6 VPN Advanced Wizard - Phase 1

Phases: IKE (Internet Key Exchange) negotiation has two phases. A phase 1 exchange establishes an IKE SA (Security Association) and phase 2 (Key Exchange) uses the SA to negotiate SAs for IPSec.

Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Negotiation Mode: Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Proposal: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.

Authentication Algorithm: **MD5** gives minimal security. **SHA-1** gives higher security.

Key Group: **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput).

SA Life Time: Set how often the ZyWALL renegotiates the IKE SA. A short SA Life Time increases security, but renegotiation temporarily disconnects the VPN tunnel.

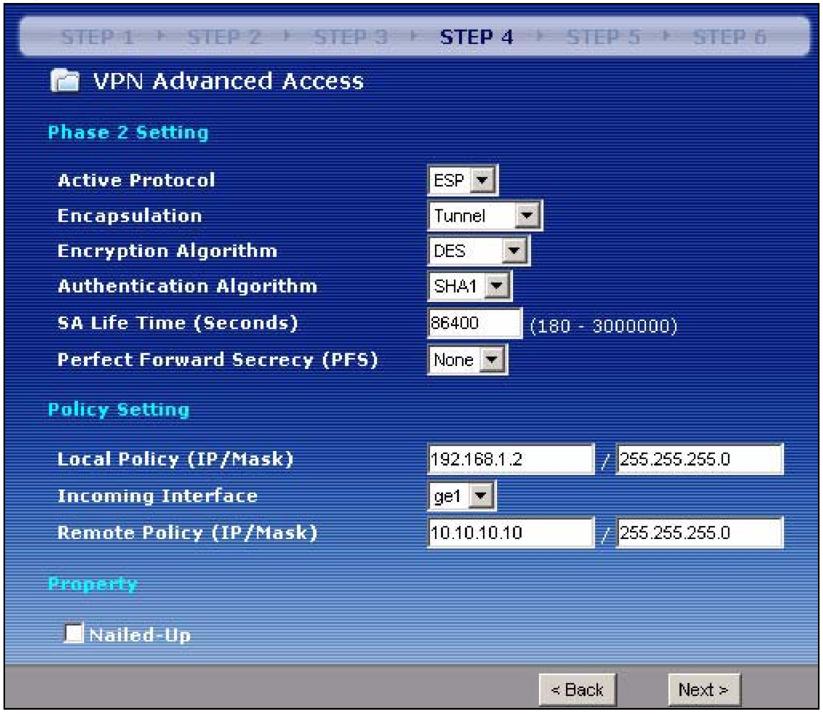
NAT Traversal: Select this if the VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices).

Use **Dead Peer Detection (DPD)** to have the ZyWALL make sure the remote IPSec router is there before transmitting data through the IKE SA. If the remote IPSec server does not respond, the ZyWALL shuts down the IKE SA.

4.8.6.1 Phase 2 Setting

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPSec.

Figure 40 VPN Advanced Wizard: Step 4



VPN Advanced Access

Phase 2 Setting

Active Protocol: ESP
Encapsulation: Tunnel
Encryption Algorithm: DES
Authentication Algorithm: SHA1
SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): None

Policy Setting

Local Policy (IP/Mask): 192.168.1.2 / 255.255.255.0
Incoming Interface: ge1
Remote Policy (IP/Mask): 10.10.10.10 / 255.255.255.0

Property

☐ Nailed-Up

The following table describes the labels in this screen.

Table 20 VPN Advanced Wizard: Step 4

LABEL	DESCRIPTION
Phase 2 Setting	
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).
Encapsulation	**Tunnel** is compatible with NAT, **Transport** is not. **Tunnel** mode encapsulates the entire IP packet to transmit it securely. **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. **Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (AH or ESP) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. **AES128** uses a 128-bit key and is faster than **3DES**. **AES192** uses a 192-bit key and **AES256** uses a 256-bit key. Select **Null** to have no encryption.

Table 20 VPN Advanced Wizard: Step 4 (continued)

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 60 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1**, **DH2** or **DH5** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
Policy Setting	
Local Policy (IP/ Mask)	Type a static local IP address that corresponds to the remote IPSec router's configured remote IP address. To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind your ZyWALL.
Incoming Interface	Select an interface from the drop-down list box to have packets encrypted by the remote IPSec router to enter the ZyWALL via this interface.
Remote Policy (IP/ Mask)	Type a static local IP address that corresponds to the remote IPSec router's configured local IP address. To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind the remote gateway.
Property	
Nail Up	Select this if you want the ZyWALL to automatically renegotiate the IPSec SA when the SA life time expires.
Next	Click **Next** to continue.

4.8.7 VPN Advanced Wizard - Phase 2

Active Protocol: **ESP** is compatible with NAT, **AH** is not.

Encapsulation: **Tunnel** is compatible with NAT, **Transport** is not.

Proposal: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.

Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the peer IPSec device.

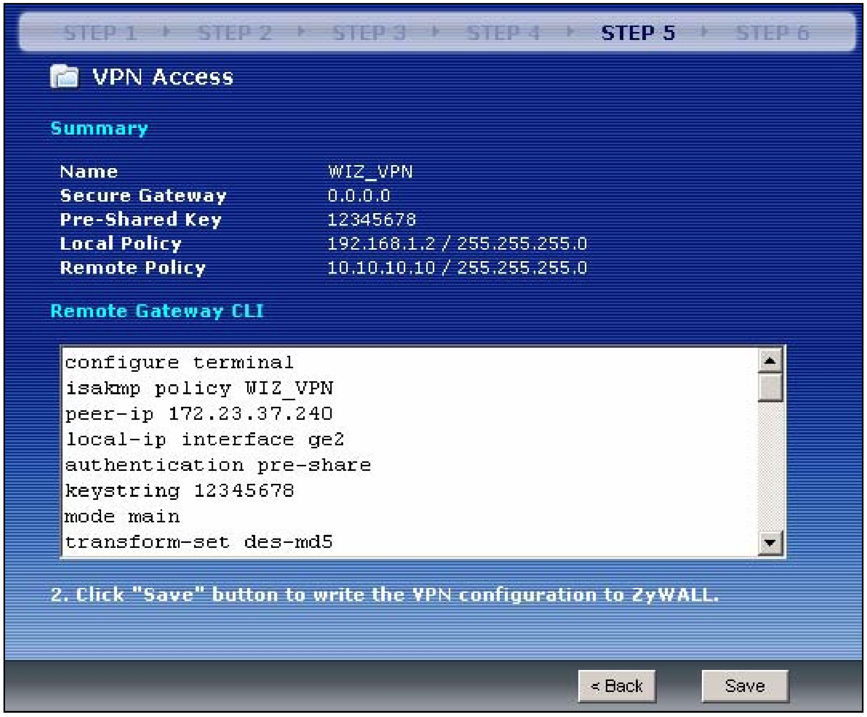
Incoming Interface: The peer IPSec device connects to the ZyWALL via this interface.

Remote Policy (IP/Mask): Type the IP address of a computer behind the peer IPSec device. You can also specify a subnet. This must match the local IP address configured on the peer IPSec device.

Nail Up: Select this to have the ZyWALL automatically renegotiate the IPSec SA when the SA life time expires.

This read-only screen shows the status of the current VPN setting. Use the summary table to check whether what you have configured is correct.

Figure 41 VPN Advanced Wizard: Step 5



Name WIZ_VPN
Secure Gateway 0.0.0.0
Pre-Shared Key 12345678
Local Policy 192.168.1.2 / 255.255.255.0
Remote Policy 10.10.10.10 / 255.255.255.0

```
configure terminal
isakmp policy WIZ_VPN
peer-ip 172.23.37.240
local-ip interface ge2
authentication pre-share
keystring 12345678
mode main
transform-set des-md5
```

2. Click "Save" button to write the VPN configuration to ZyWALL.

The following table describes the labels in this screen.

Table 21 VPN Advanced Wizard: Step 5

LABEL	DESCRIPTION
Summary	
Name	This is the name of the VPN connection (and VPN gateway).
Secure Gateway	This is the WAN IP address or domain name of the remote IPSec router. If this field displays **0.0.0.0**, only the remote IPSec router can initiate the VPN connection.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
Local Policy	This is a (static) IP address and Subnet Mask on the LAN behind your ZyWALL.
Remote Policy	This is a (static) IP address and Subnet Mask on the network behind the remote IPSec router.
Remote Gateway CLI	These commands set the matching VPN connection settings for the remote gateway. If the remote gateway is a ZLD-based ZyWALL, you can copy and paste this list into its command line interface in order to configure it for the VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.
Save	Click **Save** to store the VPN settings on your ZyWALL.

4.8.8 VPN Advanced Wizard - Summary

This summary of VPN tunnel settings is read-only.

Name: Identifies the VPN connection (and the VPN gateway).

Secure Gateway: IP address or domain name of the peer IPSec device.

Pre-Shared Key: VPN tunnel password.

Local Policy: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.

Remote Policy: IP address and subnet mask of the computers on the network behind the peer IPSec device that can use the tunnel.

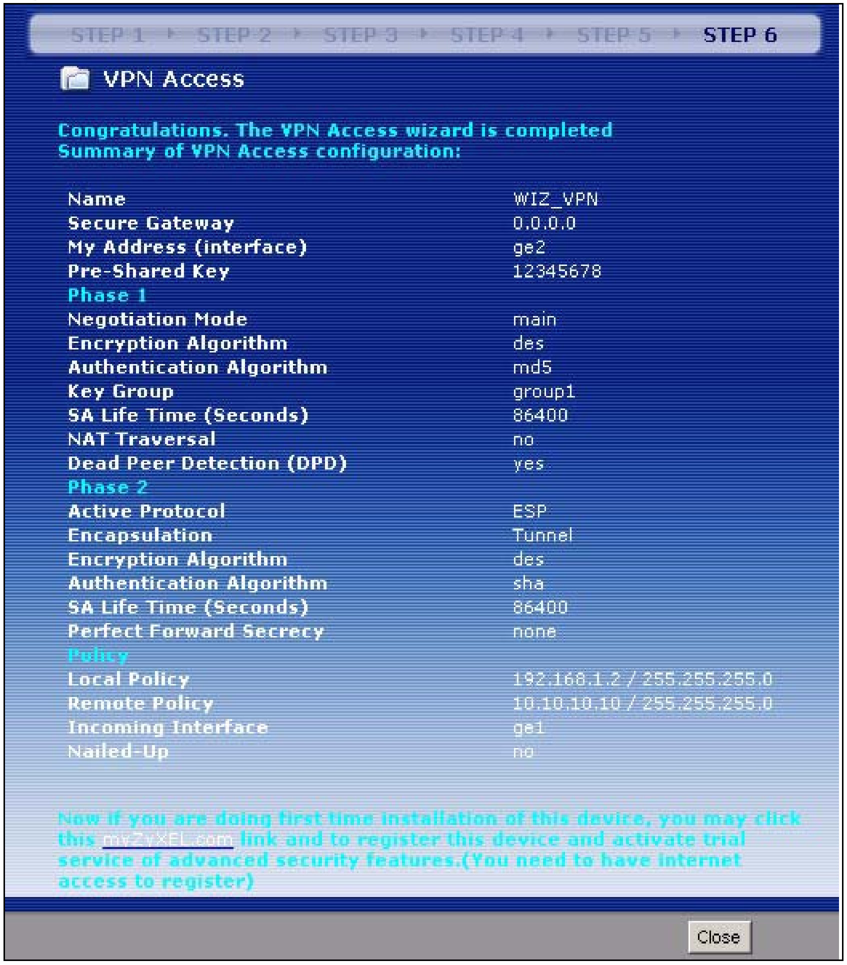
Copy and paste the **Remote Gateway CLI** commands into another ZLD-based ZyWALL's command line interface.

Click **Save** to save the VPN rule.

4.8.9 VPN Advanced Wizard - Finish

Now you can use the VPN tunnel.

Figure 42 VPN Wizard: Step 6: Advanced



Congratulations. The VPN Access wizard is completed
Summary of VPN Access configuration:

Name	WIZ_VPN
Secure Gateway	0.0.0.0
My Address (interface)	ge2
Pre-Shared Key	12345678
Phase 1	
Negotiation Mode	main
Encryption Algorithm	des
Authentication Algorithm	md5
Key Group	group1
SA Life Time (Seconds)	86400
NAT Traversal	no
Dead Peer Detection (DPD)	yes
Phase 2	
Active Protocol	ESP
Encapsulation	Tunnel
Encryption Algorithm	des
Authentication Algorithm	sha
SA Life Time (Seconds)	86400
Perfect Forward Secrecy	none
Policy	
Local Policy	192.168.1.2 / 255.255.255.0
Remote Policy	10.10.10.10 / 255.255.255.0
Incoming Interface	ge1
Nailed-Up	no

Now if you are doing first time installation of this device, you may click this myZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)

If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

You can click **Next** and use the following screen to perform a basic registration (see Section 4.4 on page 91). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

5

Configuration Basics

This section provides information to help you configure the ZyWALL effectively. Some of it is helpful when you are just getting started. Some of it is provided for your reference when you configure various features in the ZyWALL.

- Section 5.1 on page 111 introduces (very briefly) how granular the configuration is in the ZyWALL.
- Section 5.2 on page 112 introduces some differences in terminology and organization between the ZyWALL and other routers, particularly ZyNOS routers.
- Section 5.3 on page 112 explains the differences between physical ports, interfaces, and zones in the ZyWALL.
- Section 5.4 on page 114 identifies the features you should configure before and after you configure the main screens for each feature. For example, if you want to configure a trunk for load-balancing, you should configure the member interfaces before you configure the trunk. After you configure the trunk, you should configure a policy route for it as well. (You might also have to configure criteria for the policy route.)
- Section 5.5 on page 122 identifies the features (such as the criteria in a policy route, mentioned above) that are primarily used to store information used by other features.
- Section 5.6 on page 123 introduces some of the tools available for system management.

5.1 Granular Configuration

ZyWALL configuration is granular. When you configure a feature, you can often reuse settings that you have already configured (in one screen) in other screens. These reusable settings are called objects.

For example, when you set up a policy route, each criterion is an object. You can use criterion that you have already configured or select **Create Object** to configure new criteria. Any objects that you create in this screen, you can reuse --without configuring them again--in other policy routes or in other features such as firewall rules or remote management.

For a list of common objects, see Section 5.5 on page 122.

5.2 Terminology in the ZyWALL

This section highlights some differences in terminology or organization between the ZyWALL and other routers, particularly ZyNOS routers.

Table 22 ZyWALL Terminology That is Different Than ZyNOS

ZYNOS FEATURE / TERM	ZYWALL FEATURE / TERM
Port forwarding	Virtual server
IP alias	Virtual interface
Gateway policy	VPN gateway
Network policy (IPSec SA)	VPN connection

Table 23 ZyWALL Terminology That Might Be Different Than Other Products

FEATURE / TERM	ZYWALL FEATURE / TERM
Destination NAT (DNAT)	Virtual server
Source NAT (SNAT)	Policy route
Hub-and-spoke VPN	(VPN) concentrator

Table 24 NAT: Differences Between the ZyWALL and ZyNOS

ZYNOS FEATURE / SCREEN	ZYWALL FEATURE / SCREEN
Port forwarding	Virtual server
Trigger port, port triggering	Policy route
Address mapping	Policy route
Address mapping (VPN)	IPSec VPN

Table 25 Bandwidth Management: Differences Between the ZyWALL and ZyNOS

ZYNOS FEATURE / SCREEN	ZYWALL FEATURE / SCREEN
Interface bandwidth (outbound)	Interface
OSI level-7 bandwidth	Application patrol
General bandwidth	Policy route

5.3 Physical Ports, Interfaces, and Zones

If you want to configure the ZyWALL effectively, you should understand the differences between physical ports, interfaces, and zones. The following illustration provides an overview of the relationship between physical ports, interfaces, and zones in the ZyWALL. It also identifies the types of features you can configure with each one.

Table 26 Physical Ports, Interfaces, and Zones

Zones (LAN, DMZ, WAN, ...)	Used in firewall, IDP, remote management, anti-virus, ADP, application patrol
Interfaces (Ethernet, VLAN,...)	Used in VPN, zones, trunks, device HA, DDNS, policy routes, static routes, HTTP redirect, application patrol, and virtual server
Physical Ports (P1, P2, P3, P4, P5)	Used in port groups.

A physical port is the place to which you connect the cable. As shown above, you do not usually configure physical ports to use various features. You configure interfaces and zones. The ZyWALL supports one-to-one, one-to-many, many-to-one, and many-to-none relationships between physical ports and interfaces.

There are many types of interfaces in the ZyWALL. In addition to being used in various features, interfaces also describe the network that is directly connected to the ZyWALL.

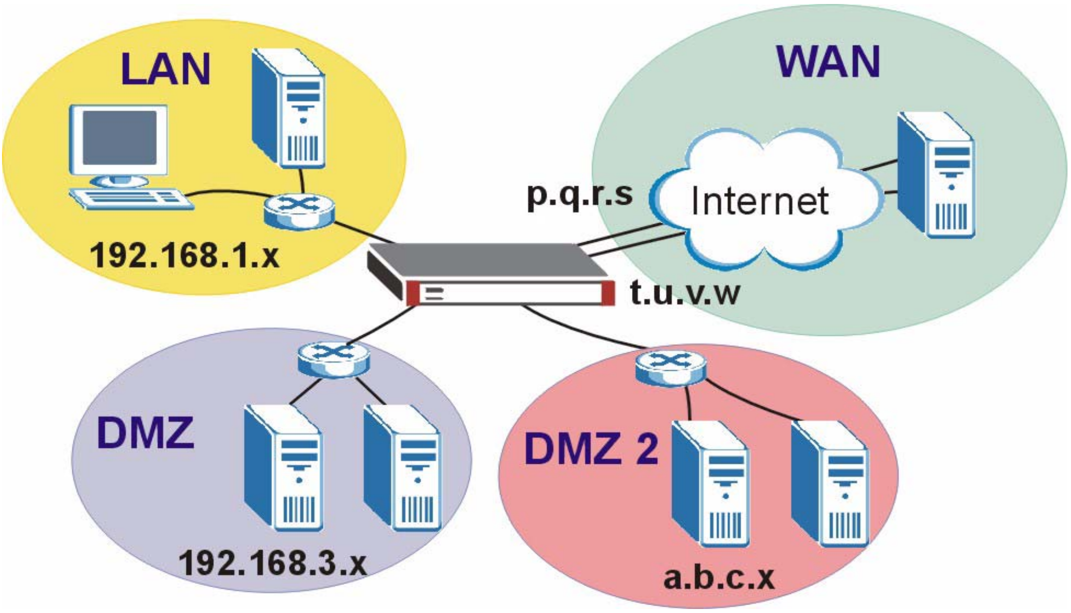
- **Port groups** create a hardware connection between physical ports at the layer-2 (MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. You also configure RIP and OSPF in these interfaces.
- **VLAN interfaces** recognize tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Then, you can configure the IP address and subnet mask of the bridge. It is also possible to configure zone-level security between the member interfaces in the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** increase the amount of routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces** (also known as IP alias), **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **AUX** port.

Zones are used for security policies. A zone is simply a group of interfaces and/or VPN tunnels; by default, the ZyWALL has LAN, WAN and DMZ zones. Each interface and VPN tunnel can be assigned to one and only one zone. You can add, change, or remove the interfaces and VPN tunnels in each zone without affecting the settings that are based on zones.

5.3.1 Network Topology Example

The following example is used to further explain the differences between interfaces and zones.

Figure 43 Interfaces and Zones: Example



- The LAN zone contains the **ge1** (Gigabit Ethernet 1) interface. This is a protected zone and uses private IP addresses. **ge1** uses 192.168.1.1 and the connected devices use IP addresses in the 192.168.1.2 to 192.168.1.254 range.
- The WAN zone contains interfaces **ge2** and **ge3**. They use public IP addresses to connect to the Internet.
- The DMZ zone contains interface **ge4**. The DMZ zone has servers that are available to the public. **ge4** uses private IP address 192.168.3.1 and the connected devices use private IP addresses in the 192.168.3.2 to 192.168.3.254 range.
- The DMZ-2 zone contains interface **ge5** and has servers that are available to the public. **ge5** and the connected servers use public IP addresses.

This example is also used in several examples in Section 5.4 on page 114.

5.4 Feature Configuration Overview

This section provides information about configuring the main features in the ZyWALL. The features are listed in the same sequence as the menu item(s) in the web configurator. Each feature is organized as shown below.

5.4.1 Feature

This provides a brief description. See the appropriate chapter(s) in this User's Guide for more information about any feature.

MENU ITEM(S)	This shows you the sequence of menu items and tabs you should click to find the main screen(s) for this feature. See the web help or the related User's Guide chapter for information about each screen.

PREREQUISITES	These are other features you should configure before you configure the main screen(s) for this feature. If you did not configure one of the prerequisites first, you can often select an option to create a new object. After you create the object you return to the main screen to finish configuring the feature. You may not have to configure everything in the list of prerequisites. For example, you do not have to create a schedule for a policy route unless time is one of the criterion.
WHERE USED	There are two uses for this. These are other features you should usually configure or check right after you configure the main screen(s) for this feature. For example, you should usually create a policy route for a VPN tunnel. You have to delete the references to this feature before you can delete any settings. For example, you have to delete (or modify) all the policy routes that refer to a VPN tunnel before you can delete the VPN tunnel.

Example: This provides a simple example to show you how to configure this feature. The example is usually based on the network topology in Figure 43 on page 114.

PREQUISITES or **WHERE USED** does not appear if there are no prerequisites or references in other features to this one. For example, no other features reference DDNS entries, so there is no **WHERE USED** entry.

5.4.2 Interface

See Section 5.3 on page 112 for background information.

When you create an interface, no security is applied on it until you assign it to a zone.

Most of the features that use interfaces support Ethernet, VLAN, bridge, and PPPoE/PPTP interfaces.

MENU ITEM(S)	**Network > Interface** (except **Network > Interface > Trunk**)
PREREQUISITES	OSPF (Ethernet interfaces), ISP accounts (PPPoE/PPTP interfaces)
WHERE USED	Zones, trunks, IPSec VPN, device HA, DDNS, policy routes, static routes, HTTP redirect, virtual server, application patrol

Example: The **ge5** interface is in the DMZ-2 zone and uses a public IP address. To configure ge5's settings, click **Network** > **Interface** > **Ethernet** and then ge5's **Edit** icon.

5.4.3 Trunks

Use trunks to set up load balancing using two or more interfaces.

MENU ITEM(S)	**Network > Interface > Trunk**

PREREQUISITES	Interfaces
WHERE USED	Policy routes

Example: See Chapter 6 on page 125.

5.4.4 IPSec VPN

Use IPSec VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ZyWALL also offers hub-and-spoke VPN.

MENU ITEM(S)	**VPN > IPSec VPN**; you can also use the **VPN Setup Wizard**, which handles most of the prerequisites for you.
PREREQUISITES	Interfaces, certificates (authentication), authentication methods (extended authentication), addresses (local network, remote network, NAT), to-ZyWALL firewall, firewall
WHERE USED	Policy routes, zones, L2TP VPN

Example: See Chapter 6 on page 125.

5.4.5 SSL VPN

Use SSL VPN to provide secure network access to remote users.

MENU ITEM(S)	**VPN > SSL VPN**
PREREQUISITES	Interfaces, SSL application, users, user groups, addresses (network list, IP pool for assigning to clients, DNS and WINS server addresses), to-ZyWALL firewall, firewall
WHERE USED	Policy routes, zones

Example: See Chapter 6 on page 125.

5.4.6 L2TP VPN

Use L2TP VPN to let remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the ZyWALL.

MENU ITEM(S)	**VPN > L2TP VPN**
PREREQUISITES	Interfaces, IPSec VPN connection, certificates (authentication), authentication methods (extended authentication), addresses (local network, remote network, NAT, IP pool for assigning to clients, DNS and WINS server addresses), to-ZyWALL firewall, firewall
WHERE USED	The IPSec VPN connection used for L2TP VPN can be used in policy routes and zones

Example: See Chapter 26 on page 351.

5.4.7 Zones

See Section 5.3 on page 112 for background information. A zone is a group of interfaces and VPN tunnels. The ZyWALL uses zones, not interfaces, in many security settings, such as firewall rules and remote management.

Zones cannot overlap. Each interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

When you create a zone, the ZyWALL does not create any firewall rules, assign an IDP profile, or configure remote management for the new zone.

MENU ITEM(S)	**Network > Zone**
PREREQUISITES	Interfaces, IPSec VPN, SSL VPN
WHERE USED	Firewall, IDP, remote management, anti-virus, ADP, application patrol

Example: For example, to create the DMZ-2 zone and add **ge5** as in the network topology example, click **Network** > **Zone** and then the **Add** icon.

5.4.8 Device HA

Use device HA to create redundant backup gateways. The ZyWALL runs VRRP v2. You can only set up device HA with other ZyWALLs of the same model running the same firmware version.

MENU ITEM(S)	**Device HA**
PREREQUISITES	Interfaces (with a static IP address), to-ZyWALL firewall

Example: See Chapter 6 on page 125.

5.4.9 DDNS

Dynamic DNS maps a domain name to a dynamic IP address. The ZyWALL helps maintain this mapping.

MENU ITEM(S)	**Network > DDNS**
PREREQUISITES	Interfaces

5.4.10 Policy Routes

Use policy routes to control the routing of packets through the ZyWALL's interfaces, trunks, and VPN connections. You also use policy routes for bandwidth management (out of the ZyWALL), port triggering, and general NAT on the source address. You have to set up the criteria, next-hops, and NAT settings in other screens first.

MENU ITEM(S)	**Network > Routing > Policy Route**
PREREQUISITES	Criteria: users, user groups, interfaces (incoming), IPSec VPN (incoming), addresses (source, destination), address groups (source, destination), schedules, services, service groups Next-hop: addresses (HOST gateway), IPSec VPN, SSL VPN, trunks, interfaces NAT: addresses (translated address), services and service groups (port triggering)

Example: You have an FTP server connected to **ge 4** (in the DMZ zone). You want to limit the amount of FTP traffic that goes out from the FTP server through your WAN connection.

1 Create an address object for the FTP server (**Object** > **Address**).

2. Click **Network** > **Routing** > **Policy Route** to go to the policy route configuration screen. Add a policy route.
3. Name the policy route.
4. Select the interface that the traffic comes in through (**ge4** in this example).
5. Select the FTP server's address as the source address.
6. You don't need to specify the destination address or the schedule.
7. For the service, select **FTP**.
8. For the **Next Hop** fields, select **Interface** as the **Type** if you have a single WAN connection or **Trunk** if you have multiple WAN connections.
9. Select the interface that you are using for your WAN connection (**ge2** and **ge3** are **WAN** interfaces by default). If you have multiple WAN connections, select the trunk.
10. Specify the amount of bandwidth FTP traffic can use. You may also want to set a low priority for FTP traffic.

The ZyWALL checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that would also match the FTP traffic.

5.4.11 Static Routes

Use static routes to tell the ZyWALL about networks not directly connected to the ZyWALL.

MENU ITEM(S)	**Network > Routing > Static Route**
PREREQUISITES	Interfaces

5.4.12 Firewall

The firewall controls the travel of traffic between or within zones. You can also configure the firewall to control traffic for virtual server (port forwarding) and policy routes (NAT). You can configure firewall rules based on schedules, specific users (or user groups), source or destination addresses (or address groups) and services (or service groups). Each of these objects must be configured in a different screen.

To-ZyWALL firewall rules control access to the ZyWALL. Configure to-ZyWALL firewall rules for remote management. By default, the firewall allows any computer from the LAN zone to access or manage the ZyWALL. The ZyWALL drops packets from the WAN or DMZ zone to the ZyWALL itself, except for Device HA and VPN traffic.

MENU ITEM(S)	**Firewall**
PREREQUISITES	Zones, schedules, users, user groups, addresses (source, destination), address groups (source, destination), services, service groups

Example: Suppose you have a SIP proxy server connected to the DMZ-2 zone for VoIP calls. You could configure a firewall rule to allow VoIP sessions from the SIP proxy server on DMZ-2 to the LAN so VoIP users on the LAN can receive calls.

1. Create a VoIP service object for UDP port 5060 traffic (**Object** > **Service**).

2 Create an address object for the VoIP server (**Object** > **Address**).

3 Click **Firewall** to go to the firewall configuration.

4 Select from the **DMZ-2** zone to the **LAN** zone, and add a firewall rule using the items you have configured.
  - You don't need to specify the schedule or the user.
  - In the **Source** field, select the address object of the VoIP server.
  - You don't need to specify the destination address.
  - Leave the **Access** field set to **Allow** and the **Log** field set to **No**.

The ZyWALL checks the firewall rules in order. Make sure each rule is in the correct place in the sequence.

5.4.13 Application Patrol

Use application patrol to control which individuals can use which services through the ZyWALL (and when they can do so). You can also specify allowed amounts of bandwidth and priorities. You must subscribe to use application patrol. You can subscribe using the **Licensing** > **Registration** screens or one of the wizards.

MENU ITEM(S)	**AppPatrol**
PREREQUISITES	Registration, zones, Schedules, users, user groups, addresses (source, destination), address groups (source, destination). These are only used as criteria in exceptions and conditions.

Example: Suppose you want to allow vice president Bob to use BitTorrent and block everyone else from using it.

1 Create a user account for Bob (**User/Group**).

2 Click **AppPatrol** > **Peer to Peer** to go to the application patrol configuration screen. Click the BitTorrent application patrol entry's **Edit** icon.
  - Set the default policy's access to **Drop**.
  - Add another policy.
  - Select the user account that you created for Bob.
  - You can leave the source, destination and log settings at the default.

With this example, Bob would have to log in using his account. If you do not want him to have to log in, you might create an exception policy with Bob's computer IP address as the source.

5.4.14 Anti-Virus

Use anti-virus to detect and take action on viruses. You must subscribe to use anti-virus. You can subscribe using the **Licensing** > **Registration** screens or one of the wizards.

MENU ITEM(S)	**Anti-X > AV**
PREREQUISITES	Registration, zones

5.4.15 IDP

Use IDP to detect and take action on malicious or suspicious packets. You must subscribe to use IDP. You can subscribe using the **Licensing** > **Registration** screens or one of the wizards.

MENU ITEM(S)	**Anti-X > IDP**
PREREQUISITES	Registration, zones

5.4.16 ADP

Use ADP to detect and take action on traffic and protocol anomalies.

MENU ITEM(S)	**Anti-X > ADP**
PREREQUISITES	Zones

5.4.17 Content Filter

Use content filtering to block or allow access to specific categories of web site content, individual web sites and web features (such as cookies). You can define which user accounts (or groups) can access what content and at what times. You must have a subscription in order to use the category-based content filtering. You can subscribe using the menu item or one of the wizards.

MENU ITEM(S)	**Anti-X > Content Filter**
PREREQUISITES	Registration, addresses (source), schedules, users, user groups

Example: You can configure a policy that blocks Bill's access to arts and entertainment web pages during the workday. You must have already subscribed to the content filter service.

1. Create a user account for Bill if you have not done so already (**User/Group**).
2. Create a schedule for the work day (**Object** > **Schedule**).
3. Click **Anti-X** > **Content Filter** > **Filter Profile**. Click the **Add** icon to go to the screen where you can configure a category-based profile.
4. Name the profile and enable it.
5. Enable the external web filter service.
6. Decide what to do for matched web sites (**Block** in this example), unrated web sites and what to do when the category-based content filtering service is not available.
7. Select the **Arts/Entertainment** category (you need to click **Advanced** to display it).
8. Click **OK**.
9. Click **General** to go to the content filter general configuration screen.
10. Enable the content filter.

11 Add a policy that uses the schedule, the filtering profile and the user that you created.

5.4.18 Virtual Server (Port Forwarding)

Use this to change the address and/or port number of packets coming in from a specified interface. This is also known as port forwarding.

The ZyWALL does not check to-ZyWALL firewall rules for packets that are redirected by virtual server. It does check regular (through-ZyWALL) firewall rules.

MENU ITEM(S)	**Network > Virtual Server**
PREREQUISITES	Interfaces, addresses (HOST)

Example: Suppose you have an FTP server with a private IP address connected to a DMZ port. You could configure a virtual server rule to forwards FTP sessions from the WAN to the DMZ.

1. Click **Network > Virtual Server** to configure the virtual server. Add an entry.
2. Name the entry.
3. Select the WAN interface that the FTP traffic is to come in through (in this example, **ge2** or **ge3**.)
4. Specify the public WAN IP address where the ZyWALL will receive the FTP packets.
5. In the **Mapped IP field**, list the IP address of the FTP server. The ZyWALL will forward the packets received for the original IP address.
6. In **Mapping Type**, select **Port**.
7. Enter 21 in both the **Original** and the **Mapped Port** fields.

5.4.19 HTTP Redirect

Configure this feature to have the ZyWALL transparently forward HTTP (web) traffic to a proxy server. This can speed up web browsing because the proxy server keeps copies of the web pages that have been accessed so they are readily available the next time one of your users needs to access that page.

The ZyWALL does not check to-ZyWALL firewall rules for packets that are redirected by HTTP redirect. It does check regular (through-ZyWALL) firewall rules.

MENU ITEM(S)	**Network > HTTP Redirect**
PREREQUISITES	Interfaces

Example: Suppose you want HTTP requests from your LAN to go to a HTTP proxy server at IP address 192.168.3.80.

1. Click **Network > HTTP Redirect**.
2. Add an entry.
3. Name the entry.
4. Select the interface from which you want to redirect incoming HTTP requests (**ge1** is a **LAN** interface by default).
5. Specify the IP address of the HTTP proxy server.
6. Specify the port number to use for the HTTP traffic that you forward to the proxy server.

5.4.20 ALG

The ZyWALL's Application Layer Gateway (ALG) allows VoIP and FTP applications to go through NAT on the ZyWALL. You can also specify additional signaling port numbers.

MENU ITEM(S)	**Network > ALG**

5.5 Objects

Objects store information and are referenced by other features. If you update this information in response to changes, the ZyWALL automatically propagates the change through the features that use the object.

The following table introduces the objects. You can also use this table when you want to delete an object because you have to delete references to the object first.

Table 27 Objects

OBJECT	WHERE USED
user/group	See the User/Group section for details on users and user groups.
address	VPN connections (local / remote network, NAT), policy routes (criteria, next-hop [HOST], NAT), firewall, application patrol (source, destination), content filter, virtual server (HOST), user settings (force user authentication), address groups, remote management (System)
address group	Policy routes (criteria), firewall, application patrol (source, destination), content filter, user settings (force user authentication), address groups, remote management (System)
service, service group	Policy routes (criteria, port triggering), firewall, service groups, log (criteria)
schedule	Policy routes (criteria), firewall, application patrol, content filter, user settings (force user authentication)
AAA server	Authentication methods
authentication methods	VPN gateways (extended authentication), WWW (client authentication)
certificates	VPN gateways, WWW, SSH, FTP
ISP account	PPPoE/PPTP interfaces
SSL Application	SSL VPN

5.5.1 User/Group

Use these screens to configure the ZyWALL's administrator and user accounts. The ZyWALL provides the following user types.

Table 28 User Types

TYPE	ABILITIES
Admin	Change ZyWALL configuration (web, CLI)
Limited-Admin	Look at ZyWALL configuration (web)
User	Access network services, browse user-mode commands (CLI)

Table 28 User Types

TYPE	ABILITIES
Guest	Access network services
Ext-User	The same as a User or a Guest. The ZyWALL looks for the specific type in an external authentication server. If the type is not available, the ZyWALL applies default settings.

If you want to force users to log in to the ZyWALL before the ZyWALL routes traffic for them, you might have to configure prerequisites first.

MENU ITEM(S)	**Object > User/Group**
PREREQUISITES	Addresses, address groups, schedules. The prerequisites are only used in policies to force user authentication
WHERE USED	Policy routes, firewall, application patrol, content filter, user groups, VPN

5.6 System Management and Maintenance

This section introduces some of the management and maintenance features in the ZyWALL. Use **Host Name** to configure the system and domain name for the ZyWALL. Use **Date/Time** to configure the current date, time, and time zone in the ZyWALL. Use **Console Speed** to set the console speed. Use **Language** to select a language for the web configurator screens.

5.6.1 DNS, WWW, SSH, TELNET, FTP, SNMP, Dial-in Mgmt, Vantage CNM

Use these screens to set which services or protocols can be used to access the ZyWALL through which zone and from which addresses (address objects) the access can come. Use **Dial-in Mgmt** for a remote management connection through an external serial modem connected to the **AUX** port.

MENU ITEM(S)	**System > DNS, WWW, SSH, TELNET, FTP, SNMP, Dial-in Mgmt, Vantage CNM, Language**
PREREQUISITES	To-ZyWALL firewall, zones, addresses, address groups, certificates (WWW, SSH, FTP, Vantage CNM), authentication methods (WWW)

Example: Suppose you want to allow an administrator to use HTTPS to manage the ZyWALL from the WAN.

1. Create an administrator account (**User/Group**).
2. Create an address object for the administrator's computer (**Object > Address**).
3. Click **System > WWW** to configure the HTTP management access. Enable HTTPS and add an administrator service control entry.
    - Select the address object for the administrator's computer.
    - Select the **WAN** zone.
    - Set the action to **Accept**.

5.6.2 File Manager

Use these screens to upload, download, delete, or run scripts of CLI commands. You can manage

- Configuration files. Use configuration files to back up and restore the complete configuration of the ZyWALL. You can store multiple configuration files in the ZyWALL and switch between them without restarting.
- Shell scripts. Use shell scripts to run a series of CLI commands. These are useful for large, repetitive configuration changes (for example, creating a lot of VPN tunnels) and for troubleshooting.

You can edit configuration files and shell scripts in any text editor.

MENU ITEM(S)	**Maintenance > File Manager**

5.6.3 Licensing Registration

Use these screens to register your ZyWALL and subscribe to services like anti-virus, IDP and application patrol, more SSL VPN tunnels, and content filtering. You must have Internet access to myZyXEL.com.

MENU ITEM(S)	**Licensing > Registration**
PREREQUISITES	Internet access to myZyXEL.com

5.6.4 Licensing Update

Use these screens to update the ZyWALL's signature packages for the anti-virus, IDP and application patrol, and system protect features. You must have a valid subscription to update the anti-virus and IDP/application patrol signatures You must have Internet access to myZyXEL.com.

MENU ITEM(S)	**Licensing > Update**
PREREQUISITES	Registration (for anti-virus and IDP/application patrol), Internet access to myZyXEL.com

5.6.5 Logs and Reports

The ZyWALL provides a system log, offers two e-mail profiles to which to send log messages, and sends information to four syslog servers. It also provides statistical reports to track user activity, web site hits, virus traffic and intrusions.

MENU ITEM(S)	**Maintenance > Log, Report**

5.6.6 Diagnostics

The ZyWALL can generate a file containing the ZyWALL's configuration and diagnostic information.

MENU ITEM(S)	**Maintenance > Diagnostics**

6

Tutorials

This chapter provides some examples of using the web configurator to set up features in the ZyWALL. See also Chapter 26 on page 351 for an example of configuring L2TP.

6.1 Interfaces and Zones

The following example shows how to use port grouping, Ethernet interfaces, trunks, and zones to set up the following configuration.

Table 29 Interfaces and Zones Example

PHYSICAL PORT	ETHERNET INTERFACE	SETTINGS	TRUNK	ZONE
1	ge1	192.168.1.1/24, DHCP server	---	LAN
2	ge1	---	---	---
3	ge3	DHCP client	WAN_TRUNK	WAN
4	ge4	172.23.37.240/24	WAN_TRUNK	WAN
5	ge5	10.0.0.1/24, DHCP server	---	DMZ

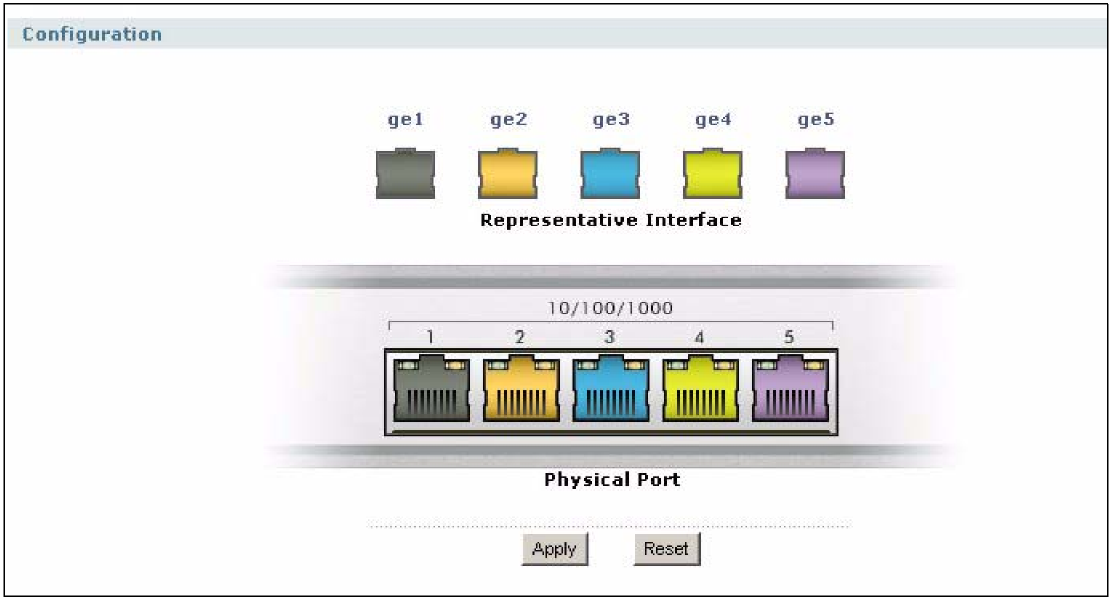
In this example, ge2 does not have any physical ports assigned to it. The example begins with the default interface configuration.

6.1.1 Set up Port Grouping

This example creates a port group in ge1 by adding physical port 2 to representative interface ge1. There are no existing port groups.

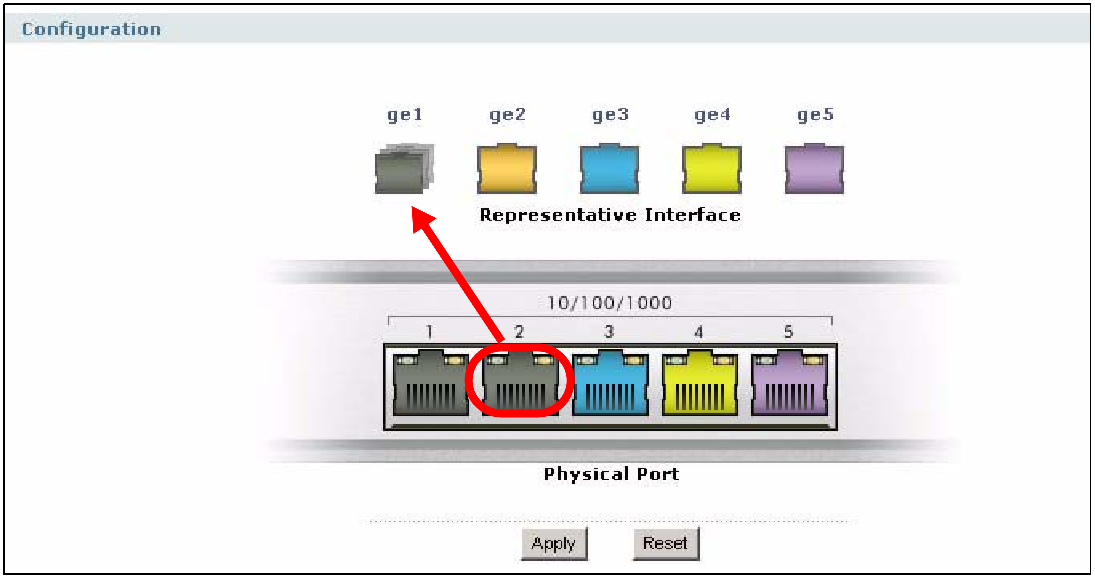
1 Click **Network** > **Interface** > **Port Grouping**. The following screen appears.

Figure 44 Network > Interface > Port Grouping, Initial


Configuration
ge1
ge2
ge3
ge4
ge5
Representative Interface
10/100/1000
1
2
3
4
5
Physical Port
Apply
Reset

2 Drag physical port **2** onto representative interface **ge1**, as shown below.

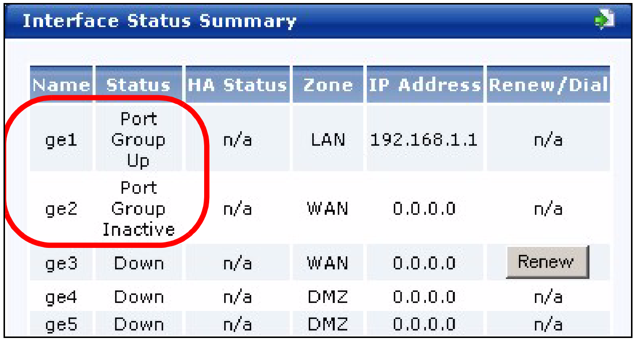
Figure 45 Network > Interface > Port Grouping, Drag-and-Drop


Configuration
ge1
ge2
ge3
ge4
ge5
Representative Interface
10/100/1000
1
2
3
4
5
Physical Port
Apply
Reset

3 Click **Apply**.

4 Click **Status**, and look at the **Interface Status Summary**, shown below. Ethernet interface ge1 has a status of **Port Group Up**, and Ethernet interface ge2 is disabled and has a **Status** of **Port Group Inactive**.

Figure 46 Status: Interface Status Summary After Port Grouping



Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	Port Group Up	n/a	LAN	192.168.1.1	n/a
ge2	Port Group Inactive	n/a	WAN	0.0.0.0	n/a
ge3	Down	n/a	WAN	0.0.0.0	Renew
ge4	Down	n/a	DMZ	0.0.0.0	n/a
ge5	Down	n/a	DMZ	0.0.0.0	n/a

6.1.2 Set up Ethernet Interfaces

This example sets up the Ethernet interfaces as shown below.

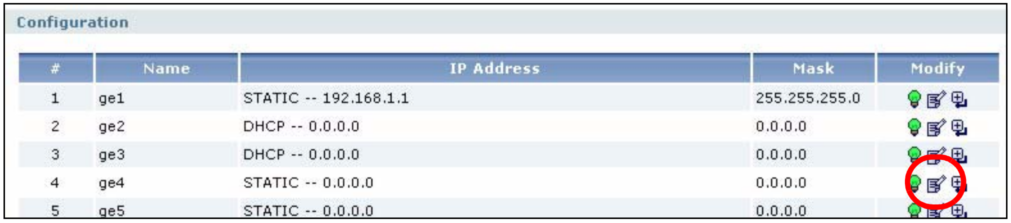
Table 30 Ethernet Interfaces Example

ETHERNET INTERFACE	SETTINGS
ge1	192.168.1.1/24, DHCP server
ge3	DHCP client
ge4	172.23.37.240/24
ge5	10.0.0.1/24, DHCP server

You have decided to use the default settings for ge1 and ge3, so it is not necessary to edit these interfaces. You can also skip ge2 because there are no physical ports associated with it anymore. Therefore, the following steps set up ge4 and ge5.

1 Click **Network** > **Interface** > **Ethernet**. The following screen appears.

Figure 47 Network > Interface > Ethernet, Initial

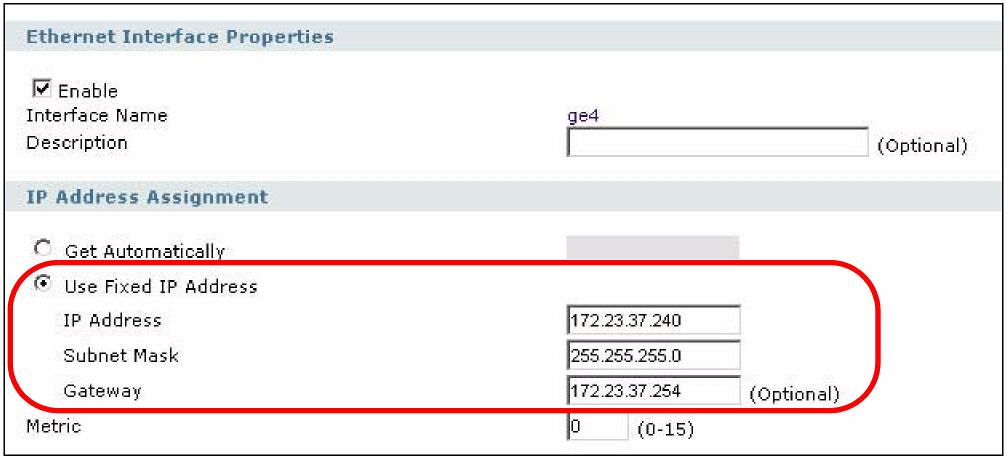


Configuration

#	Name	IP Address	Mask	Modify
1	ge1	STATIC -- 192.168.1.1	255.255.255.0	
2	ge2	DHCP -- 0.0.0.0	0.0.0.0	
3	ge3	DHCP -- 0.0.0.0	0.0.0.0	
4	ge4	STATIC -- 0.0.0.0	0.0.0.0	
5	ge5	STATIC -- 0.0.0.0	0.0.0.0	

2 Click the **Edit** icon for ge4, as shown above, and set up the IP address as shown below.

Figure 48 Network > Interface > Ethernet > ge4



Ethernet Interface Properties

☑ Enable

Interface Name	ge4
Description	(Optional)

IP Address Assignment

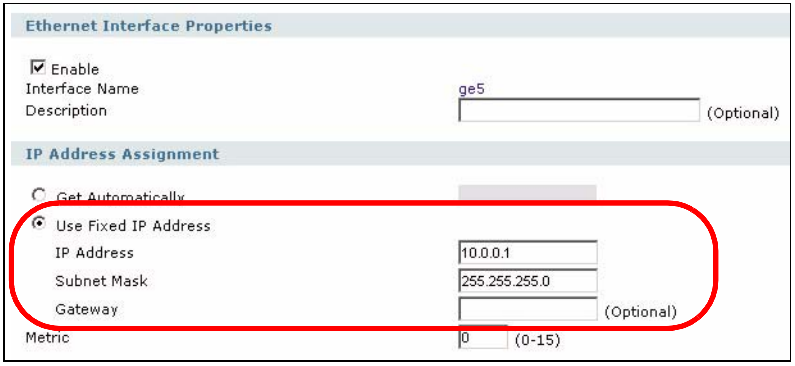
○ Get Automatically

● Use Fixed IP Address

IP Address	172.23.37.240
Subnet Mask	255.255.255.0
Gateway	172.23.37.254 (Optional)
Metric	0 (0-15)

3 Use the default values for the rest of the settings. Click **Apply** to save these changes and return to the previous screen. Click the **Edit** icon for ge5, and set up the IP address as shown below.

Figure 49 Network > Interface > Ethernet > ge5 > IP Address Assignment



Ethernet Interface Properties

☑ Enable

Interface Name	ge5
Description	(Optional)

IP Address Assignment

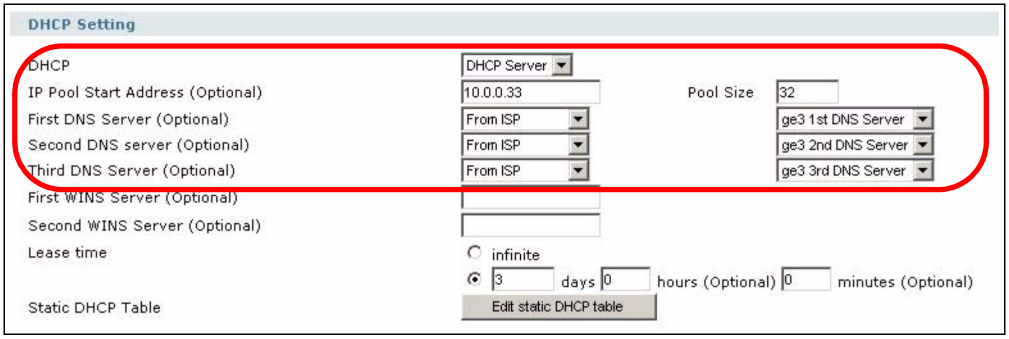
○ Get Automatically

● Use Fixed IP Address

IP Address	10.0.0.1
Subnet Mask	255.255.255.0
Gateway	(Optional)
Metric	0 (0-15)

4 Scroll down to the **DHCP Setting** section, and set up the DHCP server for ge5, as shown below.

Figure 50 Network > Interface > Ethernet > ge5 > DHCP Setting



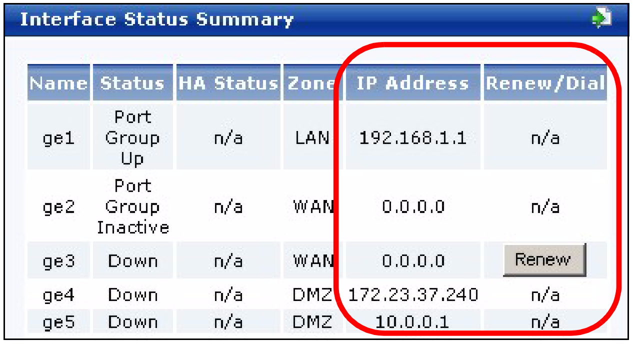
DHCP Setting

DHCP	DHCP Server		
IP Pool Start Address (Optional)	10.0.0.33	Pool Size	32
First DNS Server (Optional)	From ISP		ge3 1st DNS Server
Second DNS server (Optional)	From ISP		ge3 2nd DNS Server
Third DNS Server (Optional)	From ISP		ge3 3rd DNS Server
First WINS Server (Optional)			
Second WINS Server (Optional)			
Lease time	○ infinite ● 3 days 0 hours (Optional) 0 minutes (Optional)		
Static DHCP Table	Edit static DHCP table		

5 Use the default values for the rest of the settings. Click **Apply** to save these changes and return to the previous screen.

6 Click **Status** and look at the **Interface Status Summary**, shown below.

Figure 51 Status > Interface Status Summary, After Ethernet Interface Edits



Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	Port Group Up	n/a	LAN	192.168.1.1	n/a
ge2	Port Group Inactive	n/a	WAN	0.0.0.0	n/a
ge3	Down	n/a	WAN	0.0.0.0	Renew
ge4	Down	n/a	DMZ	172.23.37.240	n/a
ge5	Down	n/a	DMZ	10.0.0.1	n/a

6.1.3 WAN Trunk

This example sets up trunk WAN_TRUNK with ge3 and ge4. This example uses the default settings for the trunk and shows how to add the interfaces to it.

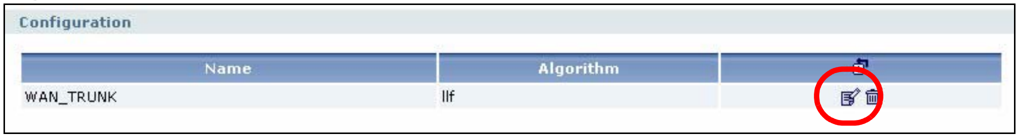
Table 31 Trunk Example

ETHERNET INTERFACE	TRUNK
ge1	---
ge3	WAN_TRUNK
ge4	WAN_TRUNK
ge5	---

There are no existing trunks at the beginning of this example.

1 Click **Network** > **Interface** > **Trunk**. The following screen appears.

Figure 52 Network > Interface > Trunk, Initial

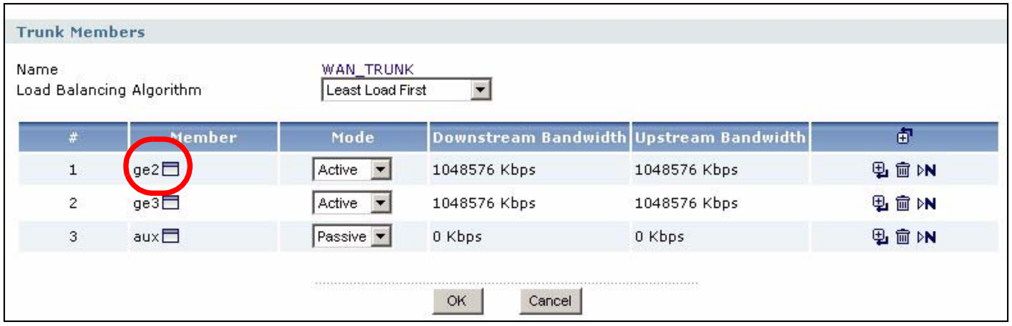


Configuration

Name	Algorithm	
WAN_TRUNK	llf	

2 Click the **Edit** icon. The following screen appears.

Figure 53 Network > Interface > Trunk > Edit, Initial



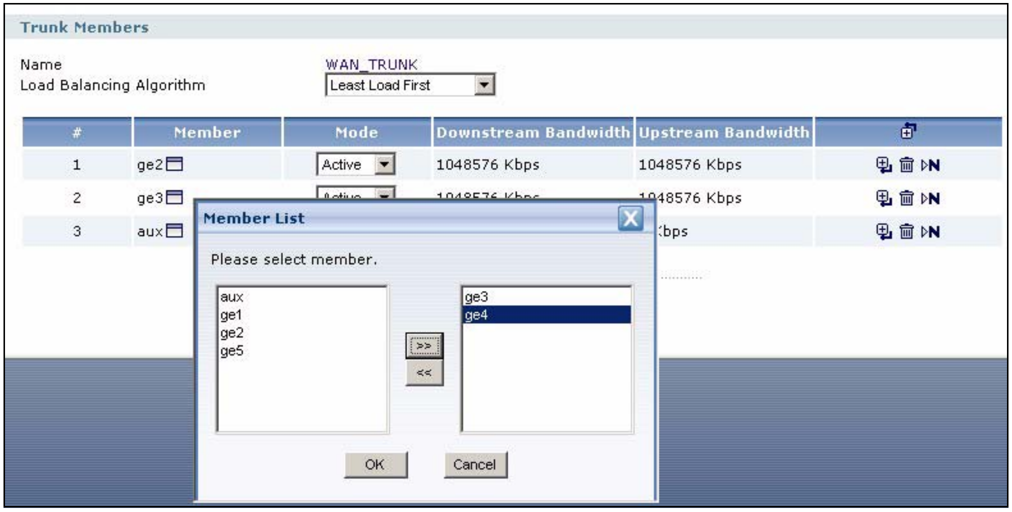
Trunk Members

Name WAN_TRUNK
Load Balancing Algorithm Least Load First

#	Member	Mode	Downstream Bandwidth	Upstream Bandwidth	
1	ge2	Active	1048576 Kbps	1048576 Kbps	
2	ge3	Active	1048576 Kbps	1048576 Kbps	
3	aux	Passive	0 Kbps	0 Kbps	

3 Click the **Member** icon, as shown above. Select the **ge2** and click the left arrow to remove it from the member list. Do the same for **aux**. Select **ge4** and click the right arrow to add it to the member list. Then click **OK**.

Figure 54 Network > Interface > Trunk > Edit > Member



Trunk Members

Name: WAN_TRUNK
Load Balancing Algorithm: Least Load First

#	Member	Mode	Downstream Bandwidth	Upstream Bandwidth
1	ge2	Active	1048576 Kbps	1048576 Kbps
2	ge3	Active	1048576 Kbps	1048576 Kbps
3	aux			

Member List

Please select member.

4 Use the default values for the rest of the settings. Click **OK** to save these changes and return to the previous screen.

6.1.4 Zones

This example sets up the LAN, WAN, and DMZ zones as shown below.

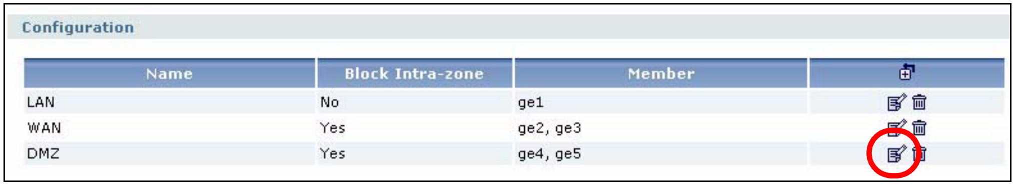
Table 32 Zones Example

ETHERNET INTERFACE	DEFAULT ZONE	FINAL ZONE
ge1	LAN	LAN
ge2	WAN	---
ge3	WAN	WAN
ge4	DMZ	WAN
ge5	DMZ	DMZ

Ethernet interface ge2 does not have any physical ports associated with it, so it does not matter to which zone it is assigned or if it is assigned to any zone at all. The only change you must make is to remove ge4 from the DMZ zone and add it to the WAN zone. The following steps accomplish this by removing ge4 from the DMZ zone and changing WAN member ge2 into ge4, leaving ge2 unassigned to any zone.

1 Click **Network** > **Zone**. The following screen appears.

Figure 55 Network > Zone, Initial

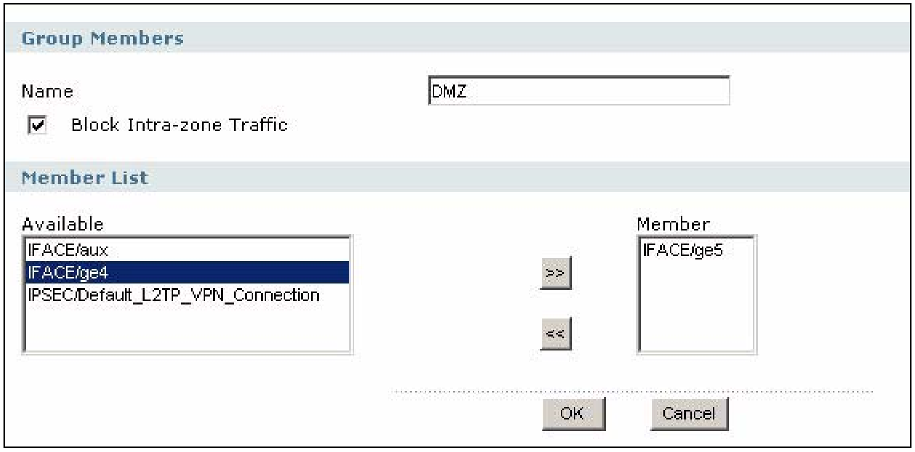


Configuration

Name	Block Intra-zone	Member
LAN	No	ge1
WAN	Yes	ge2, ge3
DMZ	Yes	ge4, ge5

2 Click the **Edit** icon for **DMZ**, as shown above because you have to remove ge4 from the DMZ before you can add it to the WAN.

Figure 56 Network > Zone > DMZ, Remove ge4



Group Members

Name: DMZ

☑ Block Intra-zone Traffic

Member List

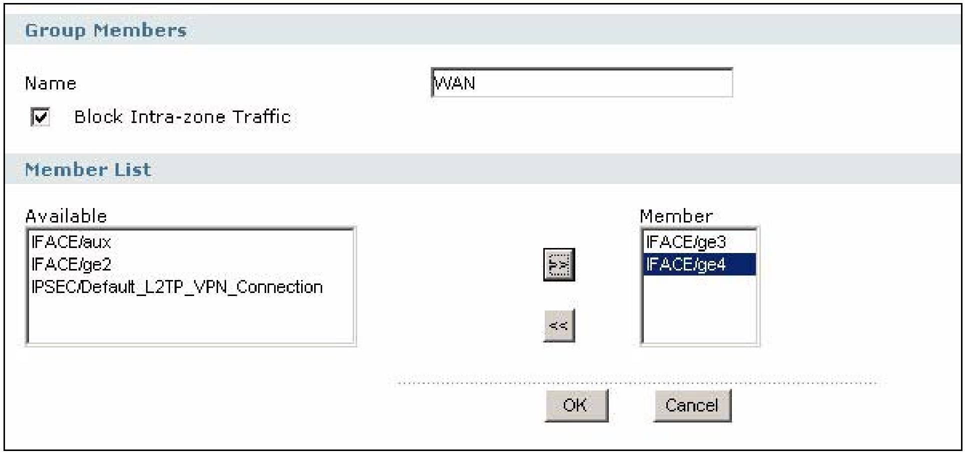
Available:
IFACE/aux
IFACE/ge4
IPSEC/Default_L2TP_VPN_Connection

Member:
IFACE/ge5

3 Select **IFACE/ge4** and click the left arrow to remove ge4 from the **Member** list. Click **OK** to save these changes and return to the previous screen.

4 Click the **Edit** icon for **WAN**. The following screen appears.

Figure 57 Network > Zone > WAN, Add ge4



Group Members

Name: WAN

☑ Block Intra-zone Traffic

Member List

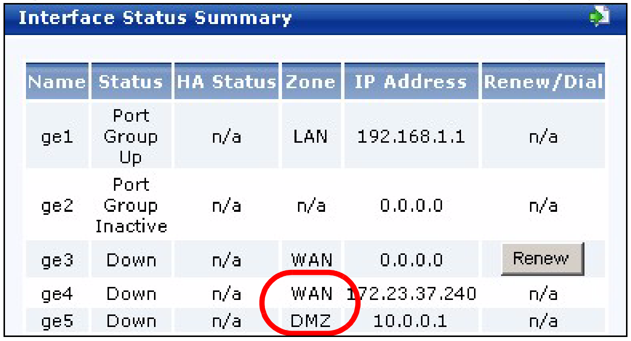
Available:
IFACE/aux
IFACE/ge2
IPSEC/Default_L2TP_VPN_Connection

Member:
IFACE/ge3
IFACE/ge4

5 Select **IFACE/ge4** and click the right arrow to add ge4 to the **Member** list. Click **OK** to save these changes and return to the previous screen.

6 Click **Status** and look at the **Interface Status Summary**, shown below.

Figure 58 Status: Interface Status Summary After Zone Edits



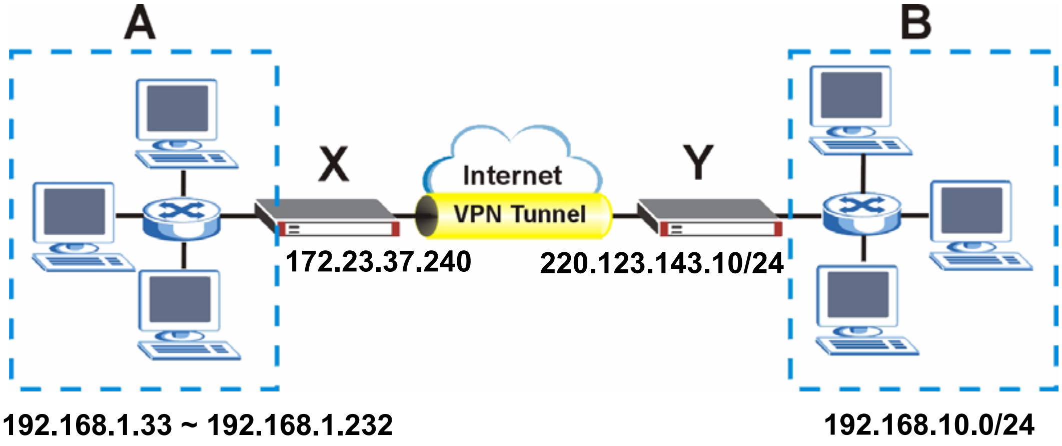
Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	Port Group Up	n/a	LAN	192.168.1.1	n/a
ge2	Port Group Inactive	n/a	n/a	0.0.0.0	n/a
ge3	Down	n/a	WAN	0.0.0.0	Renew
ge4	Down	n/a	WAN	172.23.37.240	n/a
ge5	Down	n/a	DMZ	10.0.0.1	n/a

6.2 IPSec VPN

This example is going to show you how to create the VPN tunnel illustrated below.

Figure 59 VPN Example



In this example, the ZyWALL is router **X** (172.23.37.240/24), and the remote IPSec router is router **Y** (220.123.143.10/24). Create the VPN tunnel between IP addresses 192.168.1.33 to 192.168.1.232 on our local network **A** and the remote network **B** (192.168.10.0/24).

The ZyWALL has its default settings.

6.2.1 Set up the Ethernet Interfaces and Zones

This example uses the default Ethernet interface and zone settings so they do not need to be configured.

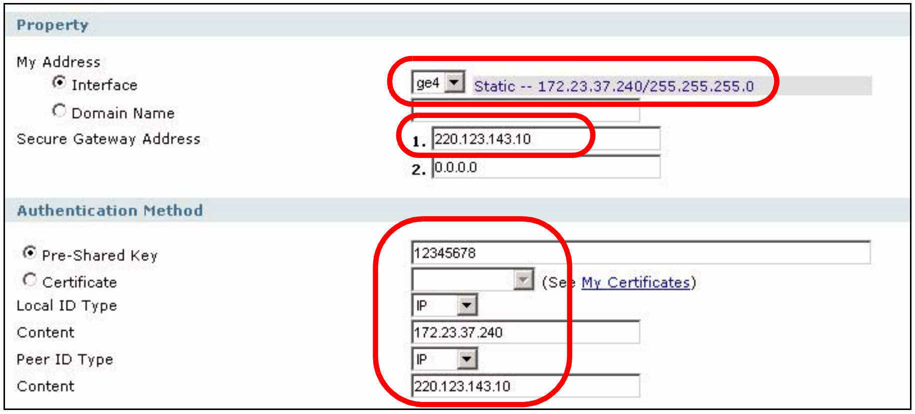
6.2.2 Set up the VPN Gateway

The VPN gateway manages the IKE SA. You do not have to set up any other objects before you configure the VPN gateway because this VPN tunnel does not use any certificates or extended authentication.

1 Click **VPN** > **IPSec VPN** > **VPN Gateway**, and then click the **Add** icon.

2 Give the VPN gateway a name ("VPN_GW_EXAMPLE"). Use the default proposal settings in this example--DES encryption, MD5 authentication, and DH1 key group. In the **Property** section, select ge4 in the **Interface** field, and enter 220.123.143.10 in the first **Secure Gateway Address** field. In the **Authentication Method** section, the pre-shared key is 12345678, and the routers are using each other's IP addresses for authentication. Click **OK**.

Figure 60 VPN > IPSec VPN > VPN Gateway > Add



My Address
● Interface: ge4 Static -- 172.23.37.240/255.255.255.0
○ Domain Name
Secure Gateway Address: 1. 220.123.143.10
2. 0.0.0.0

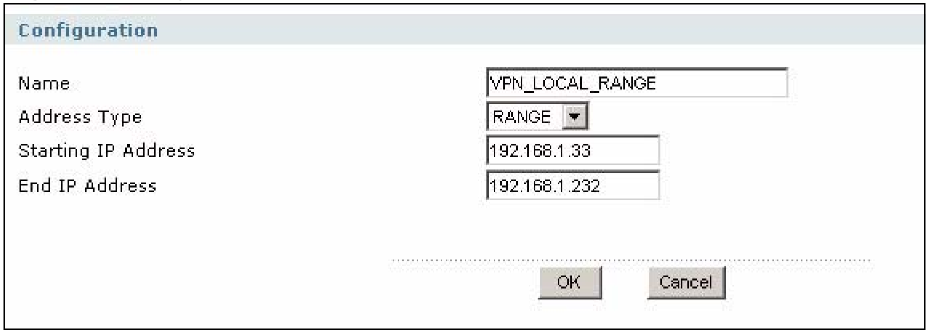
● Pre-Shared Key: 12345678
○ Certificate: (See My Certificates)
Local ID Type: IP
Content: 172.23.37.240
Peer ID Type: IP
Content: 220.123.143.10

6.2.3 Set up the VPN Connection

The VPN connection manages the IPSec SA. You have to set up the address objects for the local network and remote network before you can set up the VPN connection.

1. Click **Object** > **Address** > **Address**. Click the **Add** icon.
2. Give the new address object a name (“VPN_LOCAL_RANGE”), change the **Address Type** to **RANGE**, and set up the rest of the fields to 192.168.1.33 and 192.168.1.232. Click **OK**.

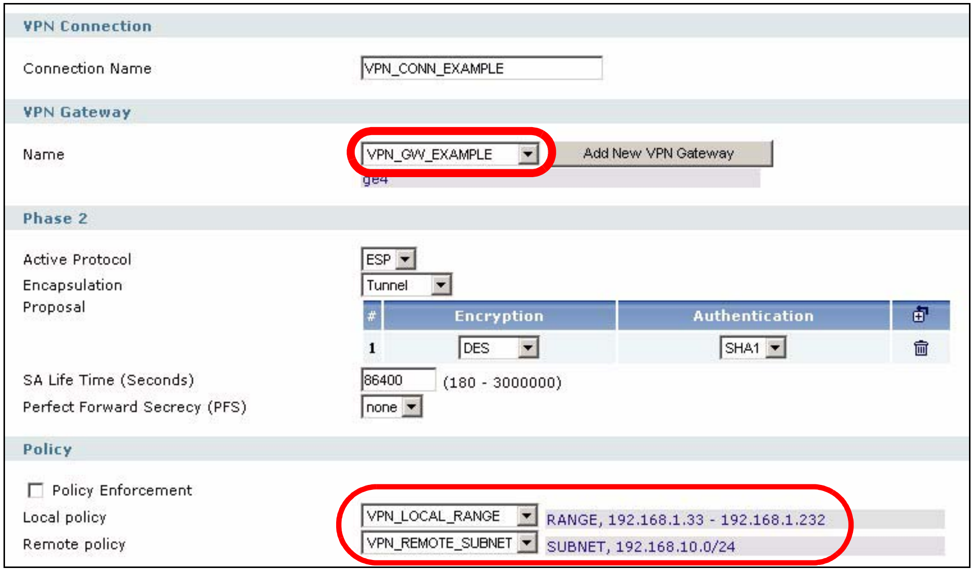
Figure 61 Object > Address > Address > Add



Name: VPN_LOCAL_RANGE
Address Type: RANGE
Starting IP Address: 192.168.1.33
End IP Address: 192.168.1.232

3. Repeat the process to create a new address object for the remote network (“VPN_REMOTE_SUBNET”, 192.168.1.0/24).
4. Click **VPN** > **IPSec VPN** > **VPN Connection**. Click the **Add** icon.
5. Give the VPN connection a name (“VPN_CONN_EXAMPLE”), and select the VPN gateway (Section 6.2.2 on page 132) in the **VPN Gateway** section. Use the default proposal settings in this example--ESP, Tunnel encapsulation, DES encryption, and SHA1 authentication--so do not change these settings. In the **Policy** section, select the address objects for the local and remote networks. Click **OK**.

Figure 62 VPN > IPSec VPN > VPN Connection > add



VPN Connection

Connection Name: VPN_CONN_EXAMPLE

VPN Gateway

Name: VPN_GW_EXAMPLE
ge4

Phase 2

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

#	Encryption	Authentication
1	DES	SHA1

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

Policy

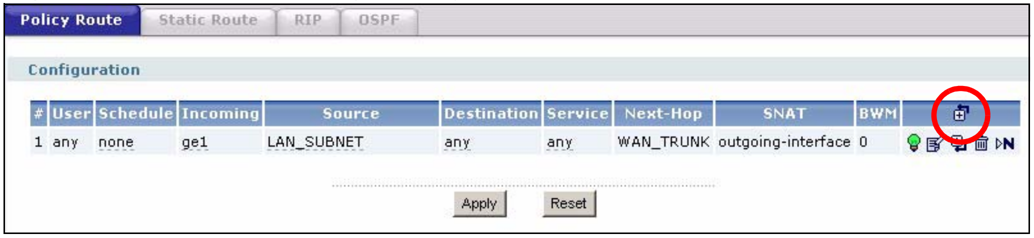
☐ Policy Enforcement
Local policy: VPN_LOCAL_RANGE RANGE, 192.168.1.33 - 192.168.1.232
Remote policy: VPN_REMOTE_SUBNET SUBNET, 192.168.10.0/24

6.2.4 Set up the Policy Route for the VPN Tunnel

You should create a new policy route to use the VPN tunnel. This policy route will only use the existing address objects, so you do not have to create any additional objects first.

1 Click **Network** > **Routing** > **Policy Route**. You want this policy route to have higher priority than the default policy route for the trunk, so click the **Add** icon at the top of the column, not the one next to the existing policy route.

Figure 63 Network > Routing > Policy Route

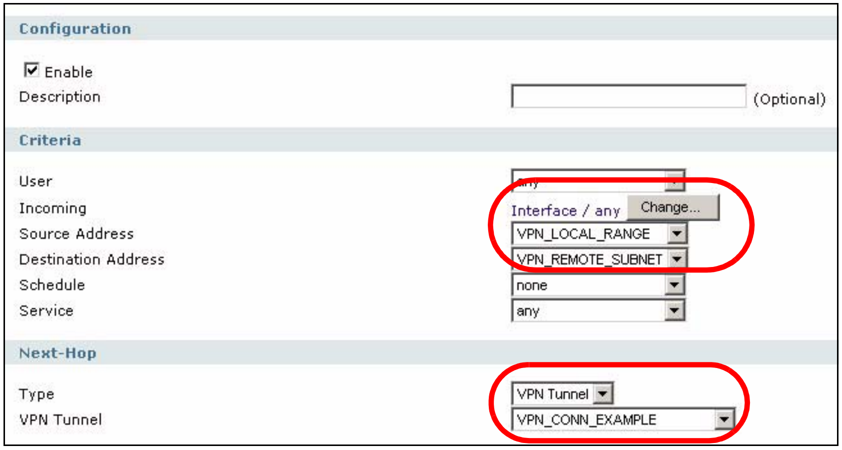


Configuration

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM
1	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0

2 Configure the policy route as shown next. This policy route applies to traffic from ge1. The source address and destination address must be the same ones represented by the address objects that you used in the VPN connection. The next-hop is the VPN connection that you created. Click **OK**.

Figure 64 Network > Routing > Policy Route > Add



Configuration

☑ Enable

Description: (Optional)

Criteria

User: any

Incoming: Interface / any Change...

Source Address: VPN_LOCAL_RANGE

Destination Address: VPN_REMOTE_SUBNET

Schedule: none

Service: any

Next-Hop

Type: VPN Tunnel

VPN Tunnel: VPN_CONN_EXAMPLE

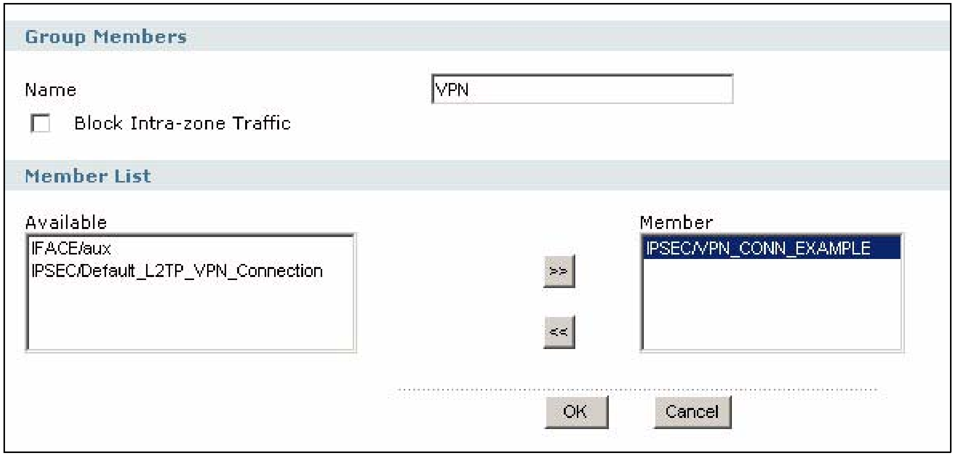
Because the new VPN connection has not been assigned to a zone yet, there are no restrictions (for example, firewall) on traffic to or from this VPN connection. You should set up the VPN settings on the remote IPSec router and try to establish the VPN tunnel before continuing.

6.2.5 Set up the Zone for the VPN Tunnel

The new VPN connection has not been assigned to a zone yet. In this example, you want to set up different security policies for VPN tunnels than you do for the default LAN, DMZ, and WAN zones, so create a new zone called VPN.

1. Click **Network** > **Zone**. Click the **Add** icon.
2. Give the zone a name ("VPN"), and add the VPN tunnel to it. Select **IPSEC/ VPN_CONN_EXAMPLE** and click the right arrow to add it to the **Member** list. Click **OK**.

Figure 65 Network > Zone > Add



Group Members

Name: VPN

☐ Block Intra-zone Traffic

Member List

Available:
IFACE/aux
IPSEC/Default_L2TP_VPN_Connection

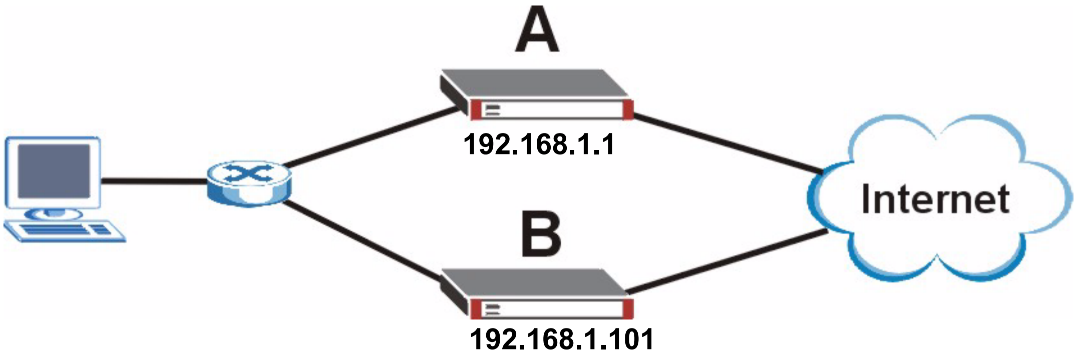
Member:
IPSEC/VPN_CONN_EXAMPLE

By default, there are no security restrictions on the new zone, so, next, you should set up security policies (firewall rules, IDP, and so on) accordingly. Make sure all the firewalls between the ZyWALL and remote IPSec router allow UDP port 500 (IKE) and IP protocol 50 (AH) or 51 (ESP). You did not enable NAT traversal, so you do not have to configure the firewalls to allow UDP port 4500.

6.3 Device HA

This example is going to show you how to set up device HA as illustrated below.

Figure 66 Device HA Example



In this example, router **A** is the default gateway for the network and uses IP address 192.168.1.1. This is the default gateway IP address for the network. There are two ZyWALL routers to ensure this gateway is available. Router **A** is the master; router **B** is the backup. Router **B** has a management IP address of 192.168.1.101.

The ZyWALL has its default settings. Configure the master first because you can synchronize the backup with the master later.

6.3.1 Set up DNS for the Virtual Router

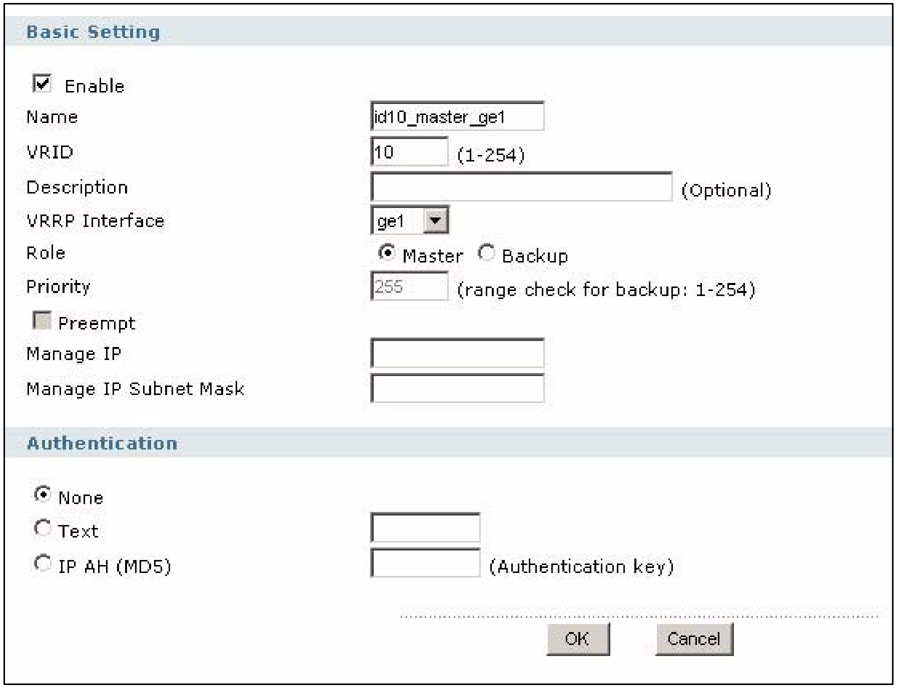
You can use a fully-qualified domain name, instead of an IP address, for the virtual router. If you want to do this, you should set up DNS before you configure the VRRP groups and synchronization. In this example, you are going to use the IP address.

6.3.2 Set up the VRRP Groups on the Master

You have to set up one VRRP group for each interface with a static IP address on which you want to set up device HA. In this example, create two VRRP groups, one for ge1 and one for ge4.

1. Click **Device HA > VRRP Group**, and then click the **Add** icon.
2. Give the VRRP group a name and virtual router ID, and select the interface ge1. This is the master router, and you are not going to use authentication. Click **OK**.

Figure 67 Device HA > VRRP Group > Add: ge1



Basic Setting

☑ Enable

Name: id10_master_ge1

VRID: 10 (1-254)

Description: (Optional)

VRRP Interface: ge1

Role: ● Master ○ Backup

Priority: 255 (range check for backup: 1-254)

☐ Preempt

Manage IP:

Manage IP Subnet Mask:

Authentication

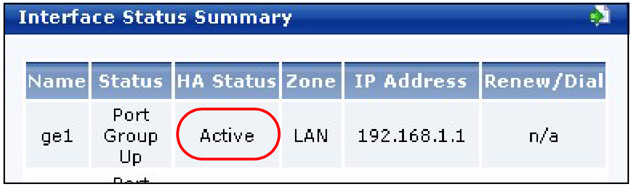
● None

○ Text

○ IP AH (MD5) (Authentication key)

3 Click **Status**, and scroll down to the **Interface Status Summary**. The **H/A Status** field is **Active**.

Figure 68 Status: Interface Status Summary: Device HA Master Configured

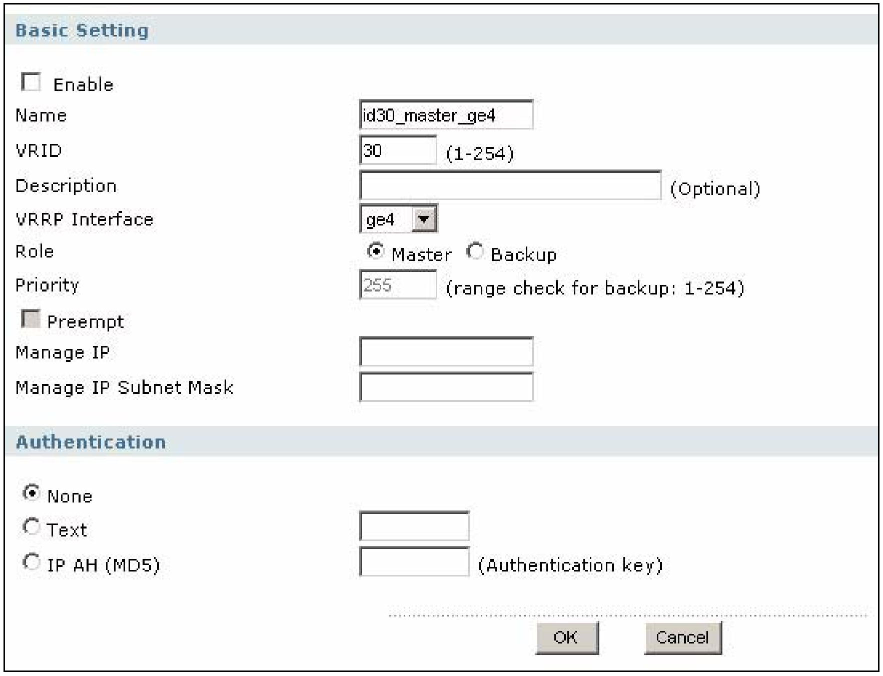


Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	Port Group Up	Active	LAN	192.168.1.1	n/a

4 Repeat these steps for the interface that is connected to the Internet. The second VRRP group should have a different VR ID. Part of an example using ge4 is shown below.

Figure 69 Network > Device HA > VRRP Group > Add: ge4



Basic Setting

☐ Enable

Name: id30_master_ge4

VRID: 30 (1-254)

Description: (Optional)

VRRP Interface: ge4

Role: ● Master ○ Backup

Priority: 255 (range check for backup: 1-254)

☐ Preempt

Manage IP:

Manage IP Subnet Mask:

Authentication

● None

○ Text

○ IP AH (MD5) (Authentication key)

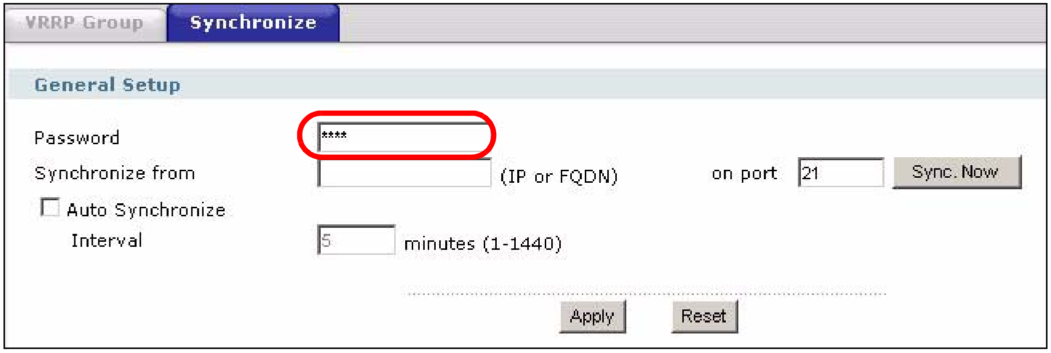
Once you configure an interface in a VRRP group, you should not configure the interface to have a dynamic IP address.

6.3.3 Set up the Password for Synchronization

1 Click **Device HA** > **Synchronize**.

2 Type the password for synchronization in the **Password** field. This password does not have to be the same as the password for the **admin** account, but you have to set the same password in the master and backup. Click **Apply**.

Figure 70 Device HA > Synchronize



General Setup

Password: ****

Synchronize from: (IP or FQDN) on port 21

☐ Auto Synchronize

Interval: 5 minutes (1-1440)

6.3.4 Finish Configuring the Master

Finish configuring the master. The backup router will get these updates later, when it synchronizes with the master.

6.3.5 Set up the Ethernet Interfaces on the Backup

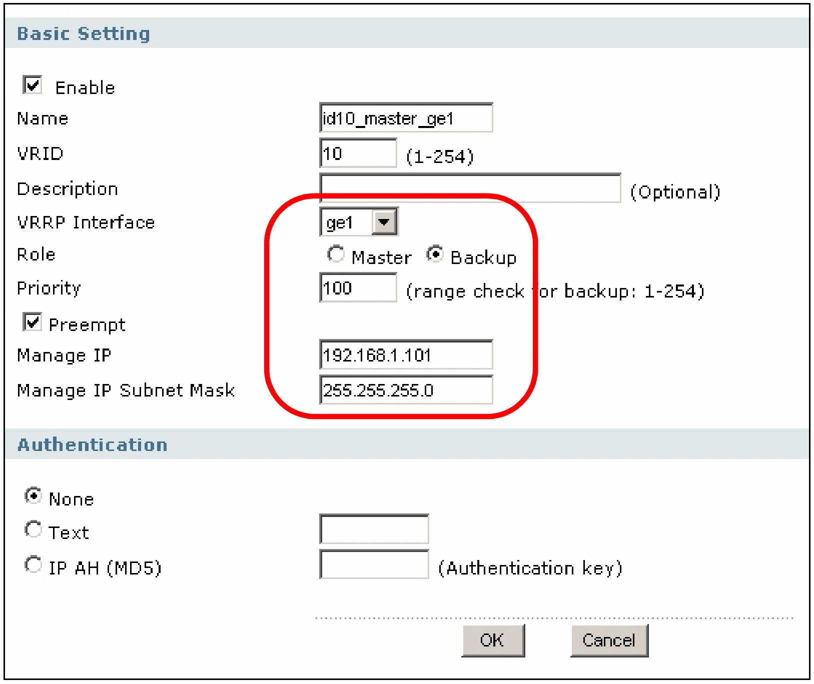
On the backup ZyWALL, ge1 should be configured exactly the same way it is configured on the master, including the same IP address. Therefore, you should not configure the backup while it is connected to the same network as the master, or there will be an IP address conflict.

You do not have to configure any other interfaces, including the one that is connected to the Internet, because the backup will get this configuration when it synchronizes with the master.

6.3.6 Set up the VRRP Groups on the Backup

You should set up the same VRRP groups on the backup that you set up on the master. The only difference is the role. In each VRRP group, select **Backup**, instead of **Master**, in the **Role** field. Therefore, you will also set up the management IP address for the backup. The VRRP group for ge1 is shown below.

Figure 71 Device HA > VRRP Group > Add



Basic Setting

☑ Enable

Name: id10_master_ge1

VRID: 10 (1-254)

Description: (Optional)

VRRP Interface: ge1

Role: ○ Master ● Backup

Priority: 100 (range check for backup: 1-254)

☑ Preempt

Manage IP: 192.168.1.101

Manage IP Subnet Mask: 255.255.255.0

Authentication

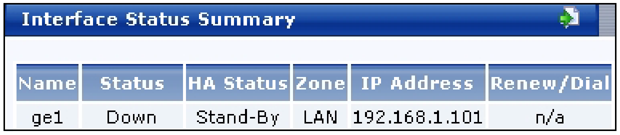
● None

○ Text

○ IP AH (MD5) (Authentication key)

Click **Status** and look at the **Interface Status Summary**. The **H/A Status** field is **Stand-By**, and the IP address is the management IP address 192.168.1.101.

Figure 72 Status: Interface Status Summary



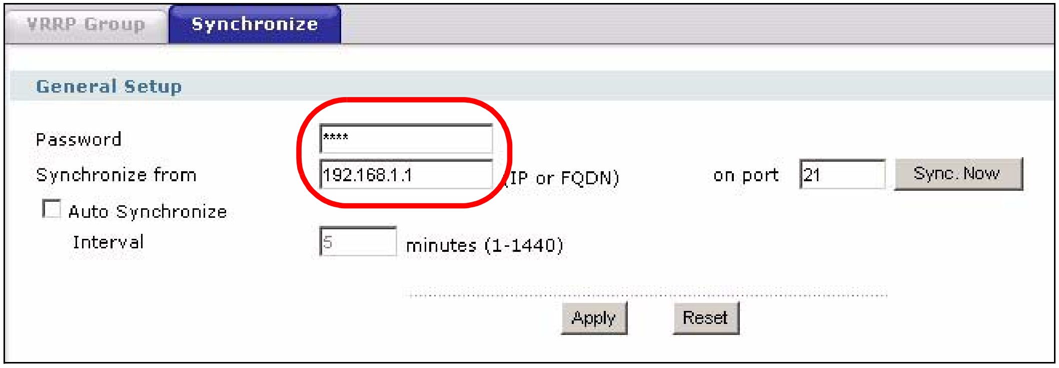
Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	Down	Stand-By	LAN	192.168.1.101	n/a

6.3.7 Synchronize the Backup

1. Connect the backup to the same network as the master.
2. Click **Device HA** > **Synchronize**.
3. Type the password for synchronization in the **Password** field. Enter the IP address of the master (on a secure network), and click **Sync Now** to get the configuration from the master.

Figure 73 Device HA > Synchronize



Password ****

Synchronize from 192.168.1.1 (IP or FQDN) on port 21

☐ Auto Synchronize

Interval 5 minutes (1-1440)

You can also set up the backup to synchronize with the master at regular intervals.

6.4 User-Aware Access Control

You can configure many policies and security settings for specific users or groups of users. This is illustrated in the following example, where you will set up the following policies. This is a simple example that does not include priorities for different types of traffic. See Section 27.4 on page 380 for more on bandwidth management.

Table 33 User-Aware Access Control Example

GROUP (USER)	WEB SURFING	WEB BANDWIDTH	MSN	LAN-TO-DMZ ACCESS
Finance (Leo)	Yes	200K	No	Yes
Engineer (Steven)	Yes	100K	No	No
Sales (Debbie)	Yes	100K	Yes (M-F, 08:30~18:00)	Yes
Boss (Andy)	Yes	100K	Yes	Yes
Guest (guest)	Yes	50K	No	No
Others	No	---	No	No

The users are authenticated by an external RADIUS server at 192.168.1.200.

First, set up the user accounts and user groups in the ZyWALL. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

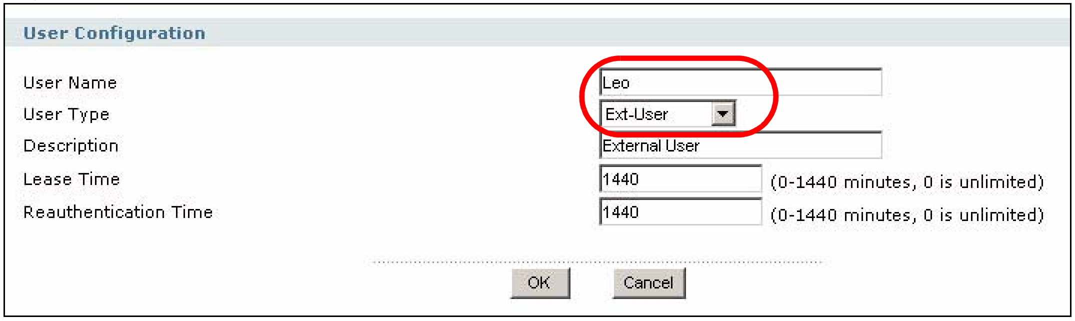
The ZyWALL has its default settings.

6.4.1 Set up User Accounts

Set up one user account for each user account in the RADIUS server. If it is possible to export user names from the RADIUS server to a text file, then you might create a script to create the user accounts instead. This example uses the web configurator.

1. Click **User/Group** > **User**. Click the **Add** icon.
2. Enter the same user name that is used in the RADIUS server, and set the **User Type** to **Ext-User** because this user account is authenticated by an external server. Click **OK**.

Figure 74 User/Group > User > Add



User Configuration

User Name: Leo
User Type: Ext-User
Description: External User
Lease Time: 1440 (0-1440 minutes, 0 is unlimited)
Reauthentication Time: 1440 (0-1440 minutes, 0 is unlimited)

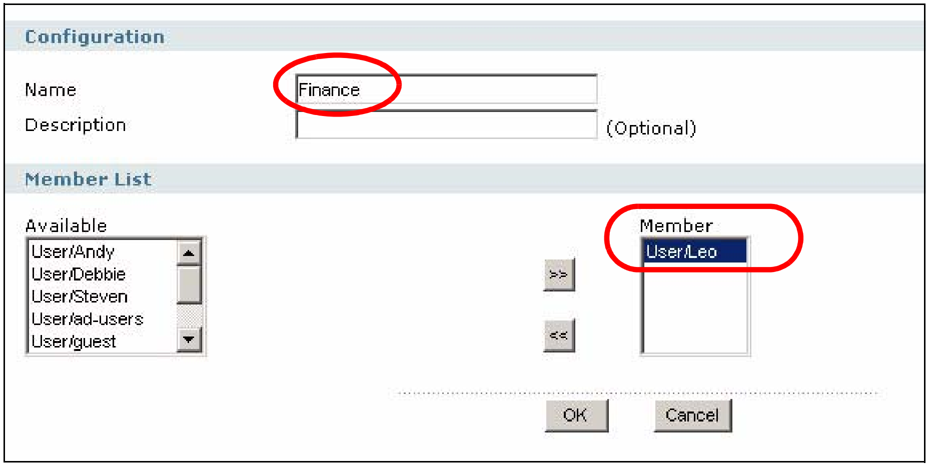
3. Repeat this process to set up the remaining user accounts.

6.4.2 Set up User Groups

Set up the user groups and assign the users to each one.

1. Click **User/Group** > **Group**. Click the **Add** icon.
2. Enter the name of the group that is used in Table 33 on page 140. In this example, it is "Finance". Then, select **User/Leo** and click the right arrow to move him to the **Member** list. This example only has one member in this group, so click **OK**. Of course you could add more members later.

Figure 75 User/Group > Group > Add



Configuration

Name: Finance
Description: (Optional)

Member List

Available: User/Andy, User/Debbie, User/Steven, User/ad-users, User/guest
Member: User/Leo

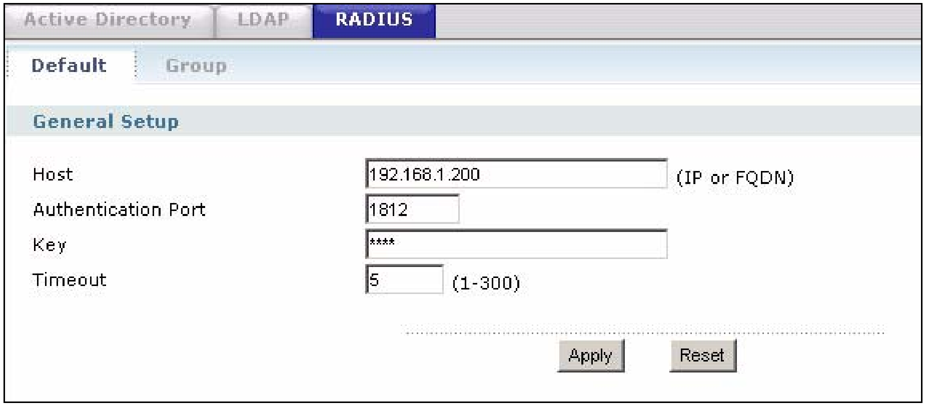
3. Repeat this process to set up the remaining user groups.

6.4.3 Set up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the ZyWALL to use the authentication method. Finally, force users to log in to the ZyWALL before it routes traffic for them.

1 Click **Object** > **AAA Server** > **RADIUS** > **Default**. Configure the RADIUS server, and click **Apply**.

Figure 76 Object > AAA Server > RADIUS > Default

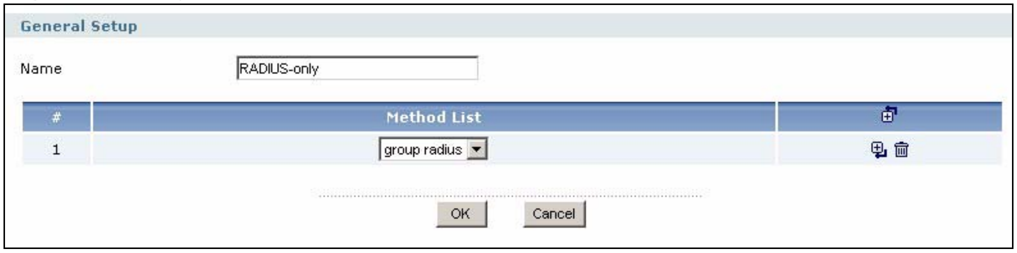


Host 192.168.1.200 (IP or FQDN)
Authentication Port 1812
Key ****
Timeout 5 (1-300)

2 Click **Object** > **Auth. method**. Click the **Add** icon.

3 Give the new authentication method a descriptive name, and click the **Add** icon. Select **group radius** because the ZyWALL should use the specified RADIUS server for authentication. Click **OK**.

Figure 77 Object > Auth. method > Add

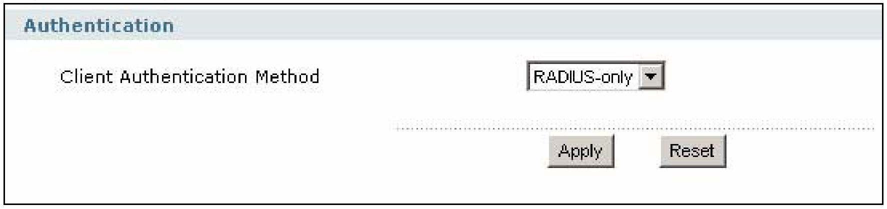


Name RADIUS-only

#	Method List
1	group radius

4 Click **System** > **WWW**. In the **Authentication** section, select the new authentication method in the **Client Authentication Method** field. Click **Apply**.

Figure 78 System > WWW > Authentication



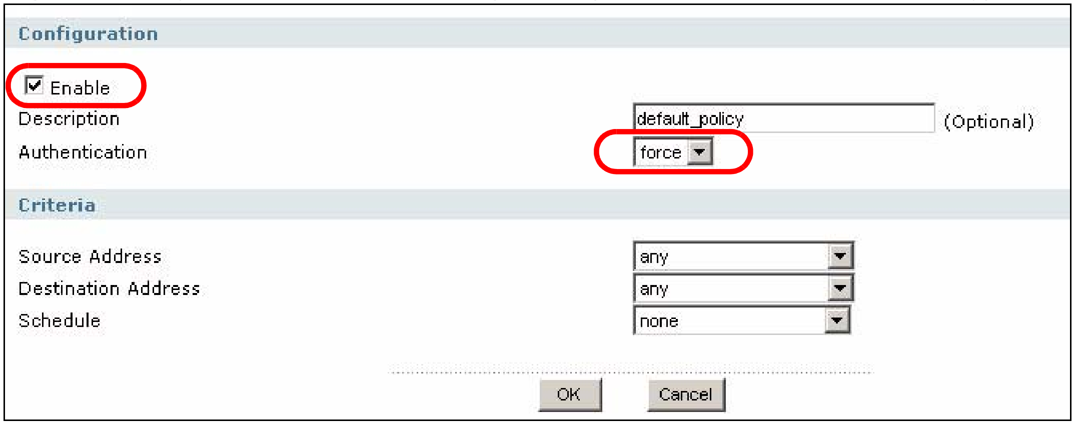
Client Authentication Method RADIUS-only

5 Click **Object** > **User/Group** > **Setting**. In the **Force User Authentication Policy** section, click the **Add** icon.

6 Set up a default policy that forces every user to log in to the ZyWALL before the ZyWALL routes traffic for them. Select **Enable**. Then, select **force** in the **Authentication** field. Keep the rest of the default settings, and click **OK**.

The users will have to log in using the web configurator login screen before they can use HTTP or MSN.

Figure 79 Object > User/Group > Setting > Add (Force User Authentication Policy)



Configuration

☑ Enable

Description: default_policy (Optional)

Authentication: force

Criteria

Source Address: any

Destination Address: any

Schedule: none

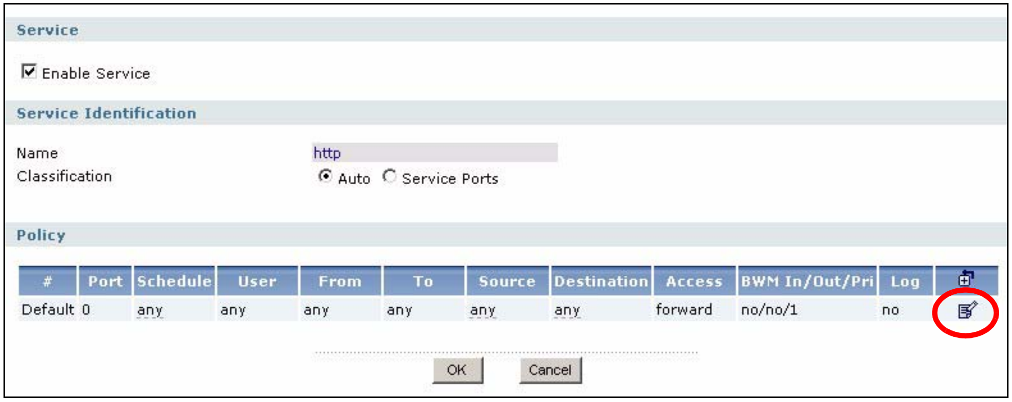
When the users try to browse the web (or use any HTTP/HTTPS application), the **Login** screen appears. They have to log in using the user name and password in the RADIUS server.

6.4.4 Set up Web Surfing Policies With Bandwidth Restrictions

Use application patrol (AppPatrol) to enforce the web surfing and MSN policies. You must have already subscribed for the application patrol service. You can subscribe using the **Licensing** > **Registration** screens or using one of the wizards.

1. Click **AppPatrol**. If application patrol is not enabled, enable it, and click **Apply**.
2. Click the **Edit** icon next to the default policy.

Figure 80 AppPatrol > http



Service

☑ Enable Service

Service Identification

Name: http

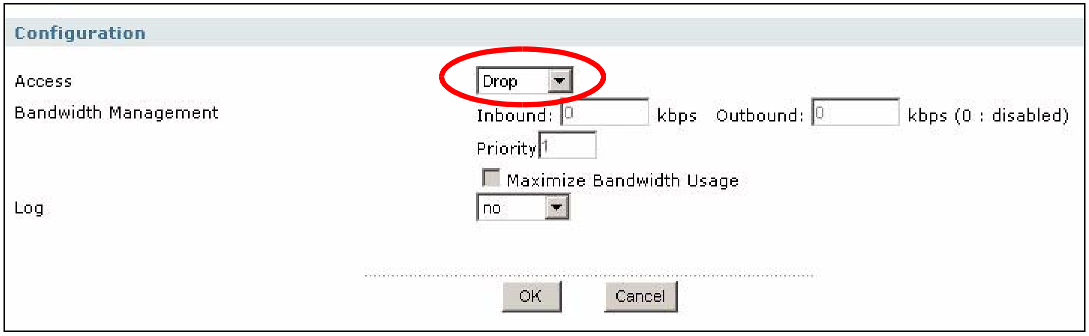
Classification: ● Auto ○ Service Ports

Policy

#	Port	Schedule	User	From	To	Source	Destination	Access	BWM In/Out/Pri	Log	
Default	0	any	any	any	any	any	any	forward	no/no/1	no	

3. Change the access to **Drop** because you do not want anyone except authorized user groups to browse the web. Click **OK**.

Figure 81 AppPatrol > http > Edit Default



Configuration

Access: Drop

Bandwidth Management: Inbound: 0 kbps Outbound: 0 kbps (0 : disabled)

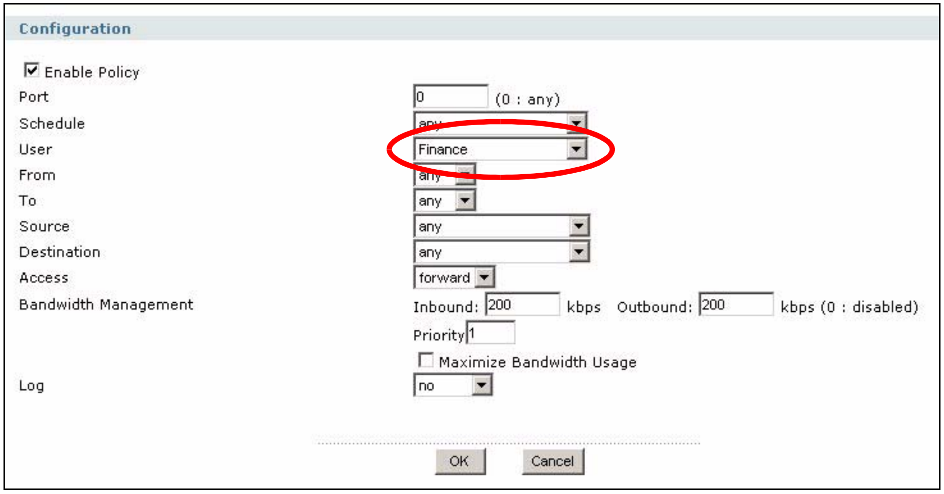
Priority: 1

☐ Maximize Bandwidth Usage

Log: no

4 Click the **Add** icon in the policy list. In the new policy, select one of the user groups that is allowed to browse the web and set the corresponding bandwidth restriction in the **Inbound** and **Outbound** fields. Click **OK**. Repeat this process to add exceptions for all the other user groups that are allowed to browse the web.

Figure 82 AppPatrol > http > Edit Default



Configuration

☑ Enable Policy

Port: 0 (0 : any)

Schedule: any

User: Finance

From: any

To: any

Source: any

Destination: any

Access: forward

Bandwidth Management: Inbound: 200 kbps Outbound: 200 kbps (0 : disabled)

Priority: 1

☐ Maximize Bandwidth Usage

Log: no

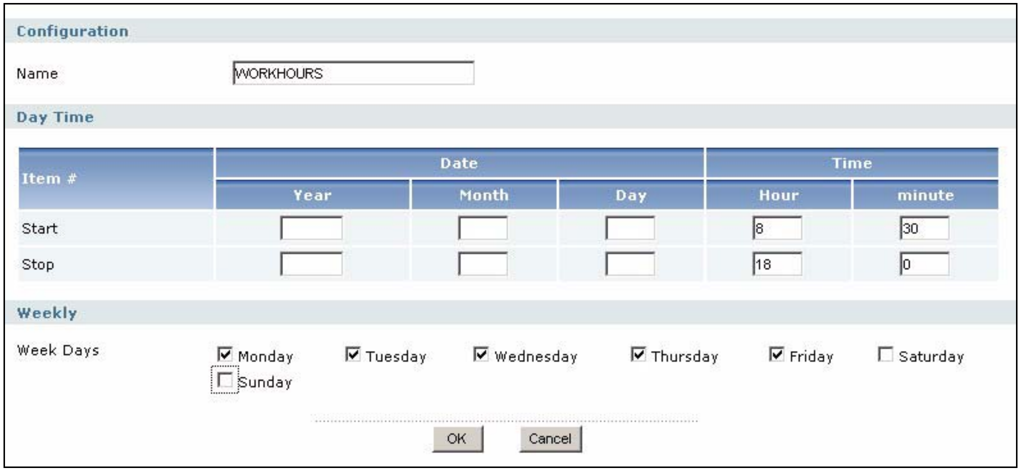
6.4.5 Set up MSN Policies

Set up a recurring schedule object first because Sales can only use MSN during specified times on specified days.

1 Click **Object** > **Schedule**. Click the **Add** icon for recurring schedules.

2 Give the schedule a descriptive name. Set up the days (Monday through Friday) and the times (8:30 - 18:00) when Sales is allowed to use MSN. Click **OK**.

Figure 83 Object > Schedule > Recurring > add



Configuration

Name: WORKHOURS

Day Time

Item #	Date			Time	
	Year	Month	Day	Hour	minute
Start				8	30
Stop				18	0

Weekly

Week Days: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☐ Saturday ☐ Sunday

3 Follow the steps in Section 6.4.4 on page 143 to set up the appropriate policies for MSN in application patrol. Make sure to specify the schedule when you configure the policy for the Sales group's MSN access.

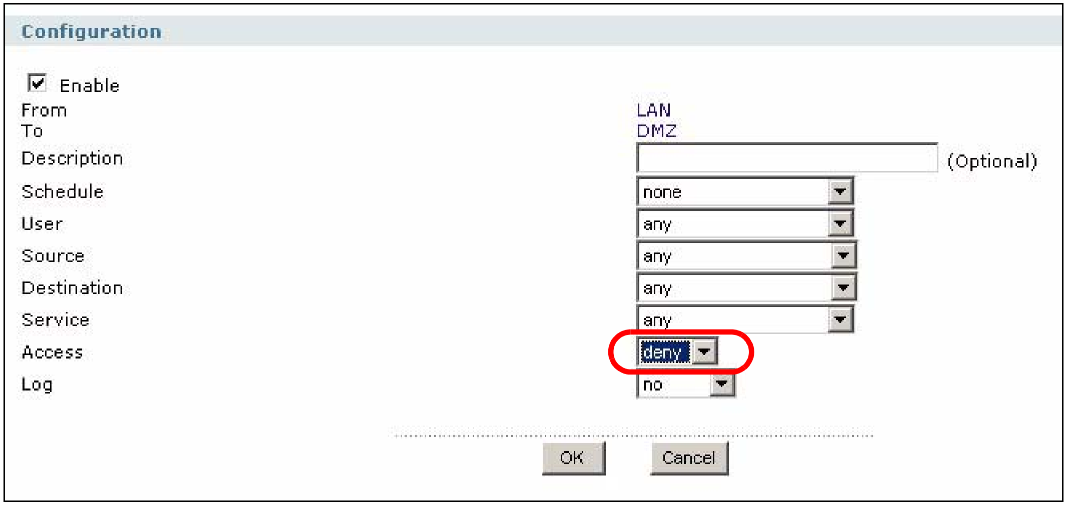
6.4.6 Set up LAN-to-DMZ Policies

Use the firewall to control access to the DMZ.

1 Click **Firewall**. In **From Zone**, select **LAN**; in **To Zone**, select **DMZ**. The default rule for LAN-to-DMZ traffic allows all traffic. You want to limit access to specific groups, so change the default rule first. Click the **Edit** icon next to it.

2 Change the **Access** field to **deny**, and click **OK**.

Figure 84 Firewall > LAN > DMZ > Edit



Configuration

☑ Enable

From: LAN

To: DMZ

Description: (Optional)

Schedule: none

User: any

Source: any

Destination: any

Service: any

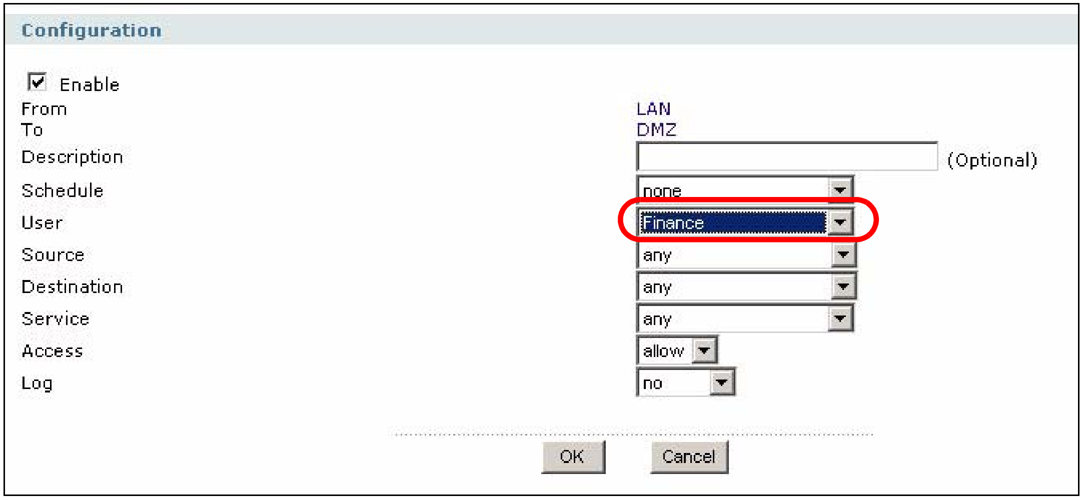
Access: deny

Log: no

3 Click the **Add** icon at the top of the rule list to create a rule for one of the user groups that is allowed to access the DMZ.

4 Select one of the user groups that is allowed to access the DMZ, and click **OK**.

Figure 85 Firewall > LAN > DMZ > Add



Configuration

☑ Enable

From: LAN

To: DMZ

Description: (Optional)

Schedule: none

User: Finance

Source: any

Destination: any

Service: any

Access: allow

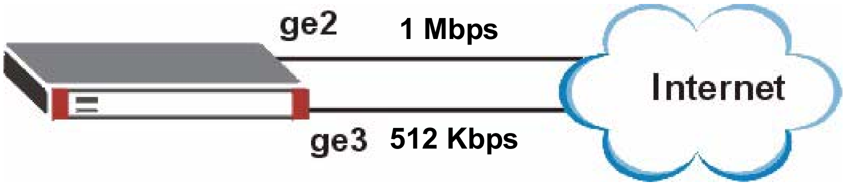
Log: no

5 Repeat this process to set up firewall rules for the other user groups that are allowed to access the DMZ.

6.5 Trunks

The following example shows how to set up a trunk for two connections (ge2 and ge3) to the Internet. The available bandwidth for each connections is 1Mbps (ge2) and 512 Kbps (ge3). As these connections have somewhat different bandwidth, you have decided to use the **Weighted Round Robin** algorithm and to send traffic to ge2 and ge3 in a 2:1 ratio.

Figure 86 Trunk Example

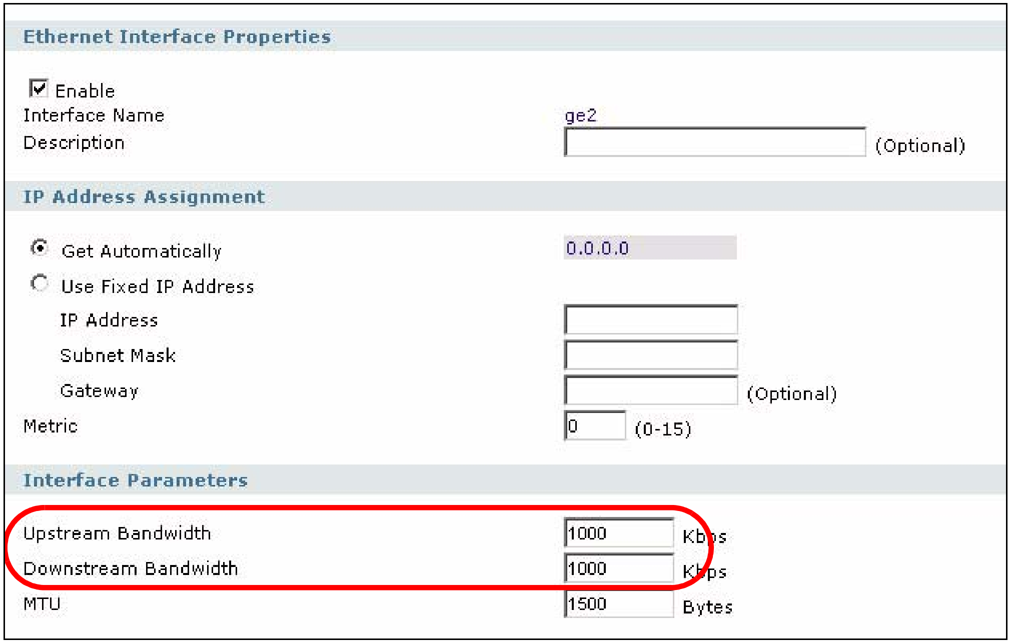


The ZyWALL has its default settings, and you do not have to change many of them to set up this trunk. You only have to set up the bandwidth on ge2 and ge3 and change the algorithm that WAN_TRUNK uses.

6.5.1 Set up Available Bandwidth on Ethernet Interfaces

1 Click **Network** > **Interface** > **Ethernet**. Click the **Edit** icon for ge2, and enter the available bandwidth (1000 kbps) in the **Upstream Bandwidth** and **Downstream Bandwidth** fields. Click **OK**.

Figure 87 Network > Interface > Ethernet > Edit > ge2



Ethernet Interface Properties

☑ Enable

Interface Name: ge2

Description: (Optional)

IP Address Assignment

● Get Automatically 0.0.0.0

○ Use Fixed IP Address

IP Address

Subnet Mask

Gateway (Optional)

Metric: 0 (0-15)

Interface Parameters

Upstream Bandwidth: 1000 Kbps

Downstream Bandwidth: 1000 Kbps

MTU: 1500 Bytes

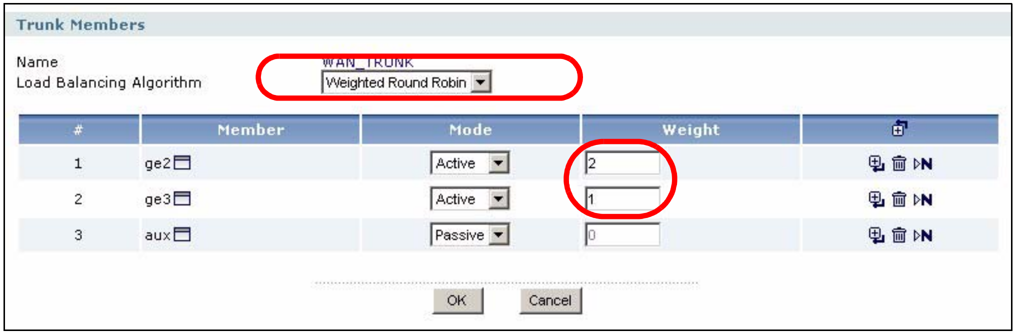
2 Click the **Edit** icon for ge3, and enter the available bandwidth (512 kbps) in the **Upstream Bandwidth** and **Downstream Bandwidth** fields. Click **OK**.

6.5.2 Change WAN Trunk Algorithm

1 Click **Network** > **Interface** > **Trunk**. Click the **Edit** icon next to WAN_TRUNK.

2 In the **Load Balancing Algorithm** field, select **Weighted Round Robin**. After the screen refreshes, enter 2 and 1 in the **Weight** column for ge2 and ge3, respectively. Click **OK**.

Figure 88 Network > Interface > Trunk > WAN_TRUNK > Edit



Trunk Members

Name: WAN_TRUNK

Load Balancing Algorithm: Weighted Round Robin

#	Member	Mode	Weight
1	ge2	Active	2
2	ge3	Active	1
3	aux	Passive	0

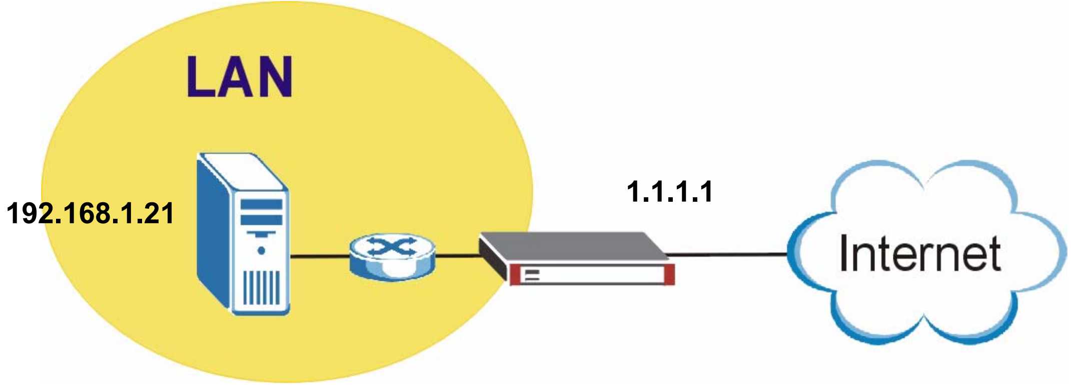
6.6 NAT 1:1 Example

In this example, there is an SMTP mail server in the LAN zone. It has a private IP address of 192.168.1.21. The public IP address of the server is 1.1.1.1.

In order for the server to be accessible to people from the Internet (WAN zone), you need to create a 1:1 NAT mapping from the public IP address to its private one.

The firewall is enabled, so you also need to create a rule to allow traffic in from the WAN zone.

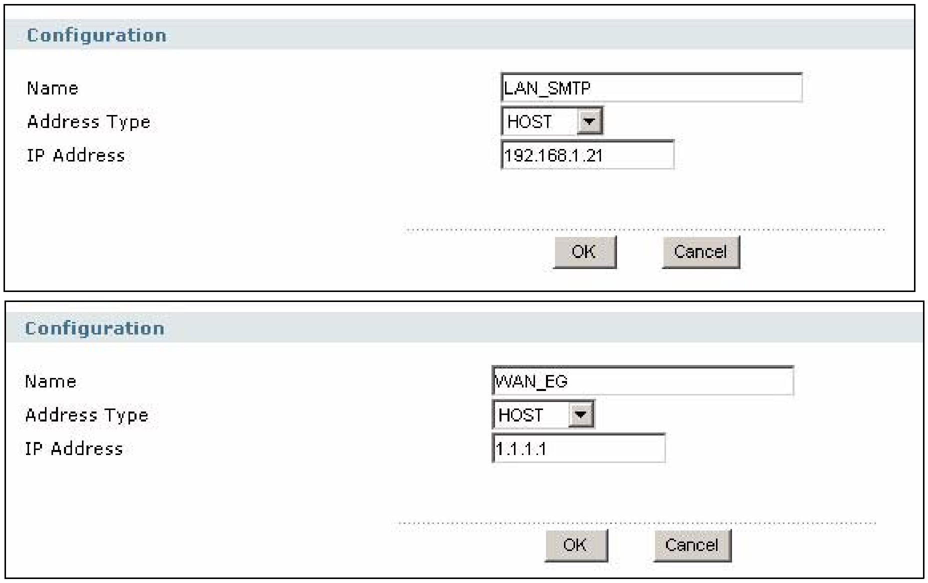
Figure 89 NAT 1:1 Example Network Topology


LAN
192.168.1.21
1.1.1.1
Internet

6.6.1 NAT 1:1 Address Objects

First create two address objects for the private and public IP addresses (LAN_SMTP and WAN_EG) in the **Object > Address** screen as shown next.

Figure 90 Create Address Objects


Configuration

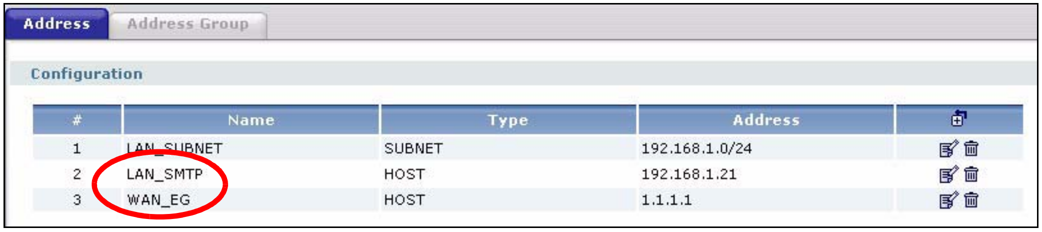
Name: LAN_SMTP
Address Type: HOST
IP Address: 192.168.1.21

OK
Cancel
Configuration

Name: WAN_EG
Address Type: HOST
IP Address: 1.1.1.1

OK
Cancel

Figure 91 Address Objects

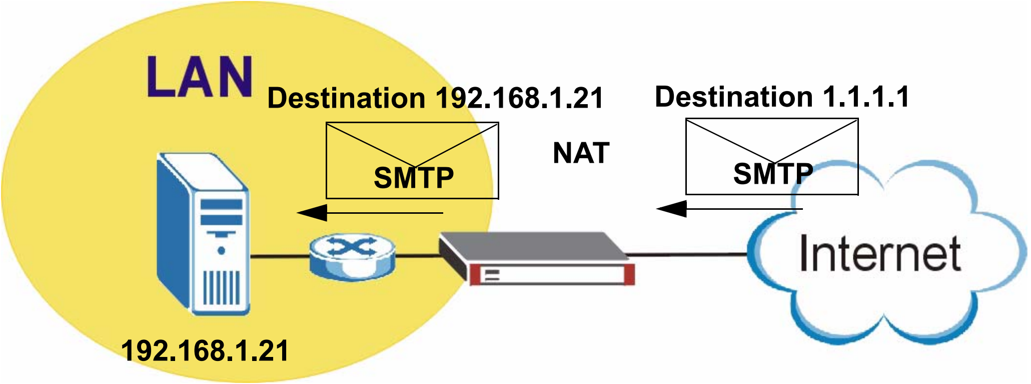

Address
Address Group
Configuration

#	Name	Type	Address	
1	LAN_SUBNET	SUBNET	192.168.1.0/24	
2	LAN_SMTP	HOST	192.168.1.21	
3	WAN_EG	HOST	1.1.1.1	

6.6.2 NAT 1:1 Virtual Server

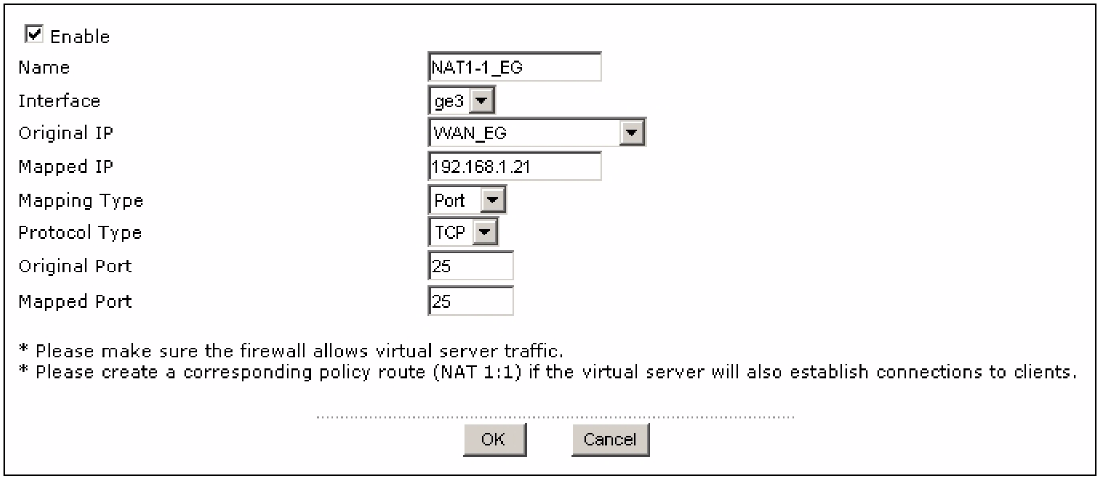
This section sets up a virtual server rule that changes the destination of SMTP traffic coming to IP address 1.1.1.1 at the ZyWALL's ge3 (WAN) interface, to the LAN SMTP server's IP address (192.168.1.21). This is also called Destination NAT (DNAT)

Figure 92 NAT 1:1 Example Virtual Server



The ge3 WAN interface has a different IP address than 1.1.1.1, so in order for the ZyWALL gateway to be able to do ARP resolution correctly, you need to create a ge3 virtual server entry. In the **Network > Virtual Server** screen, click the + symbol and create a new virtual server entry as shown next. This entry maps TCP port 25 (SMTP) traffic coming to IP address 1.1.1.1 on ge3 to the IP address of the SMTP server (192.168.1.21). In this example the SMTP server also uses port 25, so the **Mapped Port** is set to 25.

Figure 93 Create a Virtual Server



☑ Enable

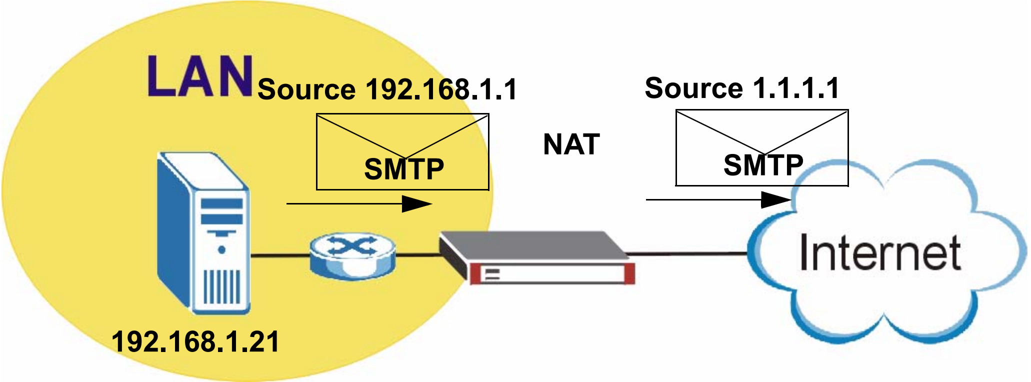
Name	NAT1-1_EG
Interface	ge3
Original IP	WAN_EG
Mapped IP	192.168.1.21
Mapping Type	Port
Protocol Type	TCP
Original Port	25
Mapped Port	25

* Please make sure the firewall allows virtual server traffic.
* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish connections to clients.

6.6.3 NAT 1:1 Policy Route

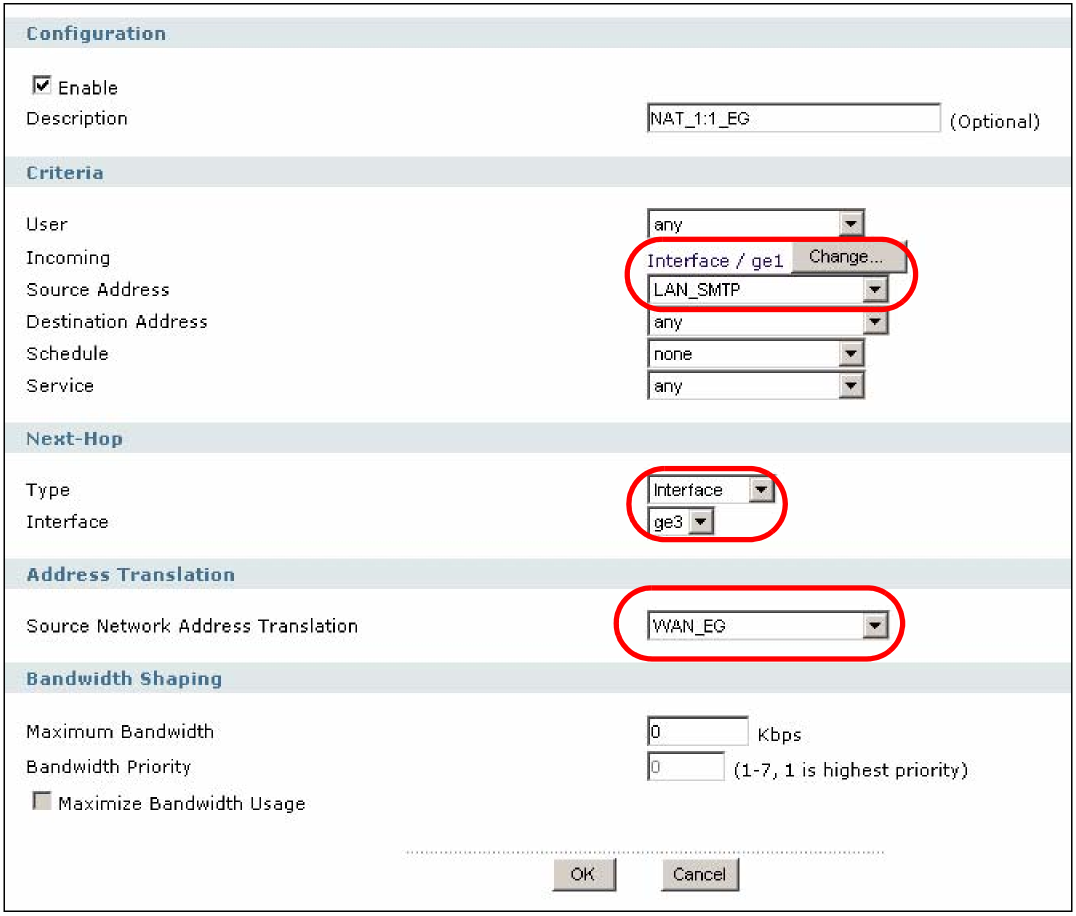
This section sets up a policy route for the traffic coming from the LAN SMTP server to the ZyWALL's ge1 (LAN) interface. It changes the source address from 192.168.1.21 to 1.1.1.1. This is also called Source NAT (SNAT). It sends the traffic out through ge3 (a WAN interface).

Figure 94 NAT 1:1 Example Policy Route



Click **Network** > **Routing** > **Policy Route** > **Add** and configure the screen as shown next. Be careful of where you create the route as routes are ordered in descending priority.

Figure 95 Create a Policy Route



Configuration

☑ Enable

Description: NAT_1:1_EG (Optional)

Criteria

User: any

Incoming: Interface / ge1

Source Address: LAN_SMTP

Destination Address: any

Schedule: none

Service: any

Next-Hop

Type: Interface

Interface: ge3

Address Translation

Source Network Address Translation: WAN_EG

Bandwidth Shaping

Maximum Bandwidth: 0 Kbps

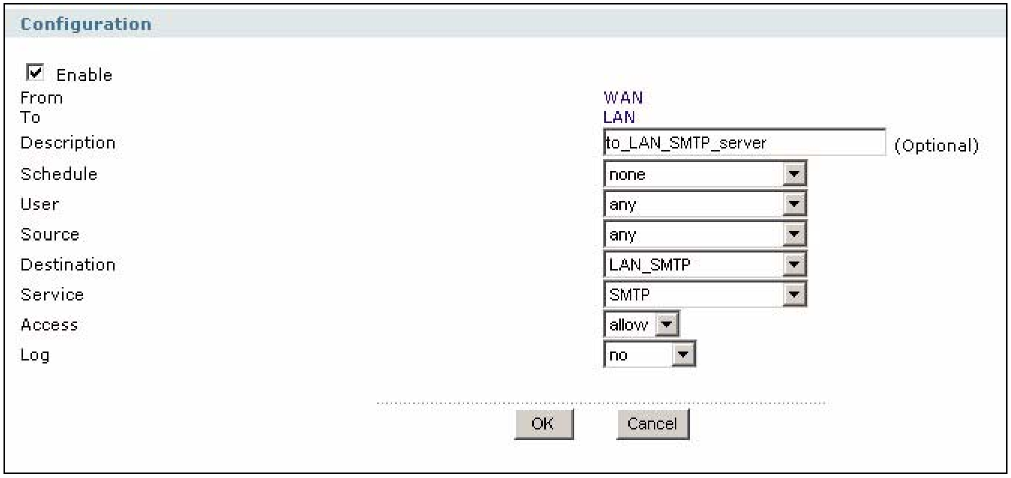
Bandwidth Priority: 0 (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

6.6.4 NAT 1:1 Firewall Rule

Create a firewall rule to allow access from the WAN zone to the mail server in the LAN zone. Be careful of where you create the rule as firewall rules are ordered in descending priority.

Figure 96 Create a Firewall Rule



Configuration

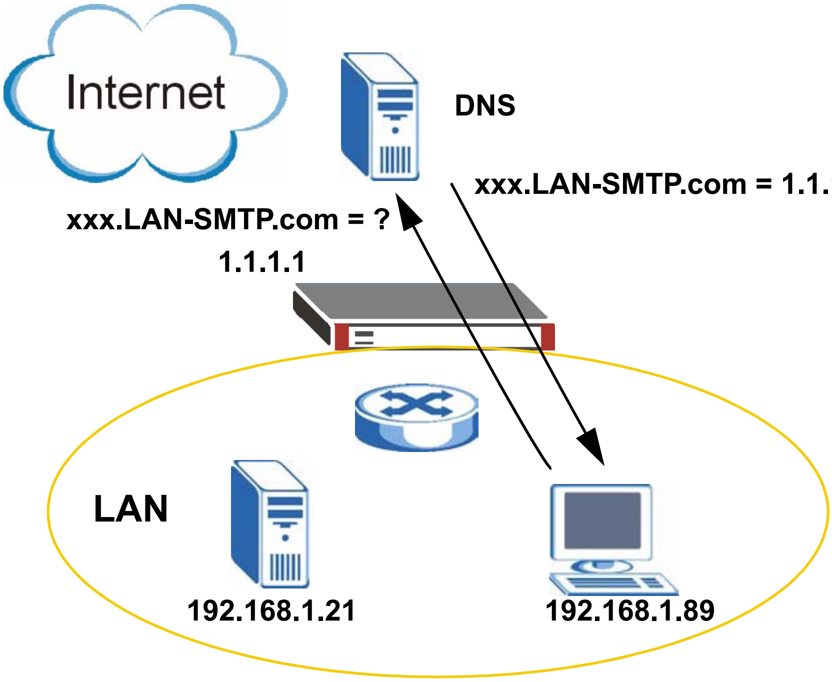
☑ Enable

From	WAN
To	LAN
Description	to_LAN_SMTP_server (Optional)
Schedule	none
User	any
Source	any
Destination	LAN_SMTP
Service	SMTP
Access	allow
Log	no

6.7 NAT Loopback

The NAT 1:1 example in Section 6.6 on page 147 maps a public IP address to the private IP address of a LAN SMTP mail server to allow users to access the SMTP mail server from the WAN. LAN users can also use an IP address to access the mail server. However, you need to configure NAT loopback for LAN users to use a domain name to access the server.

Figure 97 LAN Computer Queries the DNS Server

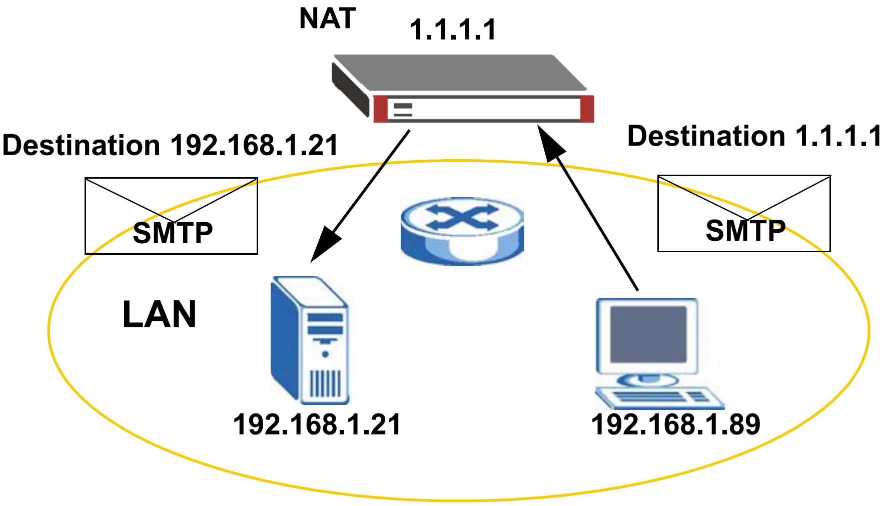


A LAN user computer at IP address 192.168.1.89 queries the domain name (xxx.LAN-SMTP.com in this example) from a public DNS server and gets the SMTP server’s 1-1 NAT mapped public IP address of 1.1.1.1.

6.7.1 NAT Loopback Virtual Server

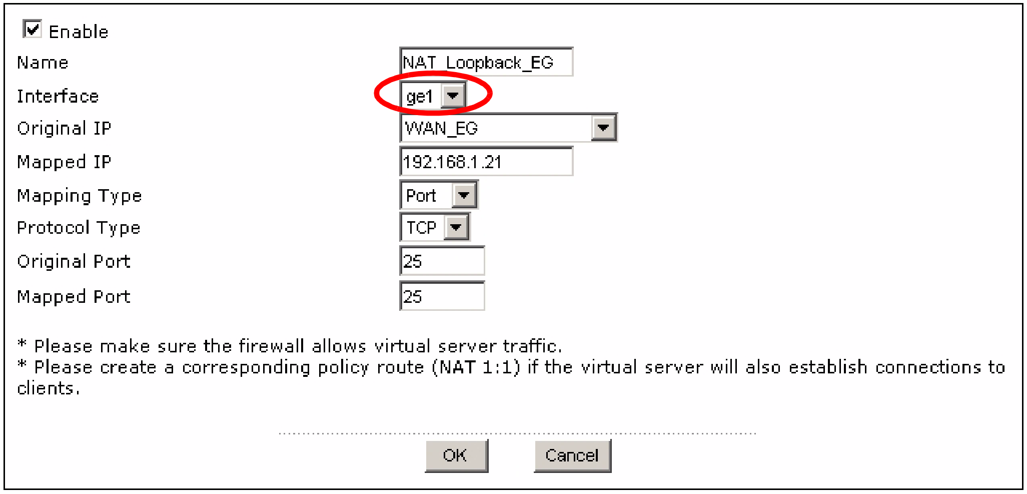
When a LAN user sends SMTP traffic to IP address 1.1.1.1, the traffic comes into the ZyWALL through the ge1 (LAN) interface, thus it does not match the NAT 1:1 mapping's virtual server rule for SMTP traffic coming to IP 1.1.1.1 from ge3 (the WAN). So you must configure a similar virtual server rule for ge1.

Figure 98 NAT Loopback Virtual Server



Click **Network** > **Virtual Server** and the + symbol and create the virtual server rule as shown next. This virtual server rule is the same as the NAT 1:1 virtual rule in Section 6.6.2 on page 149, except you use the LAN interface (ge1) instead of the WAN interface (ge3). This rule maps TCP port 25 (SMTP) traffic destined for IP address 1.1.1.1 and coming in on ge1 to the IP address of the SMTP server (192.168.1.21). In this example the SMTP server also uses port 25, so the **Mapped Port** is set to 25.

Figure 99 Create a Virtual Server



☑ Enable

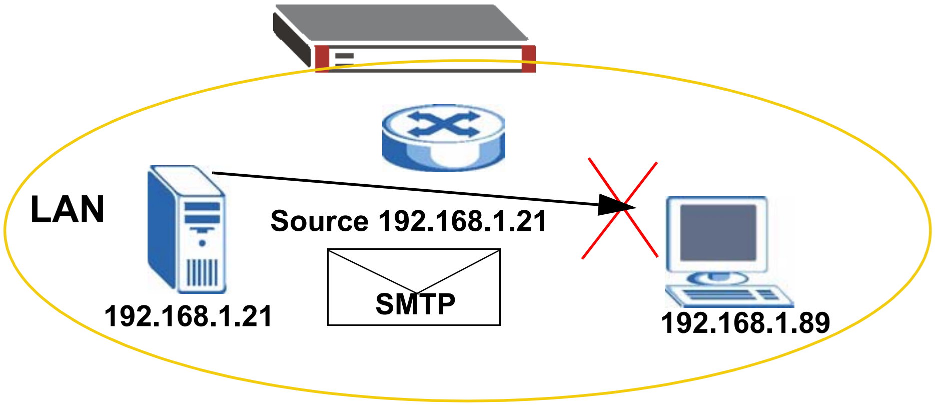
Name	NAT_Loopback_EG
Interface	ge1
Original IP	WAN_EG
Mapped IP	192.168.1.21
Mapping Type	Port
Protocol Type	TCP
Original Port	25
Mapped Port	25

* Please make sure the firewall allows virtual server traffic.
* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish connections to clients.

6.7.2 NAT Loopback Policy Route

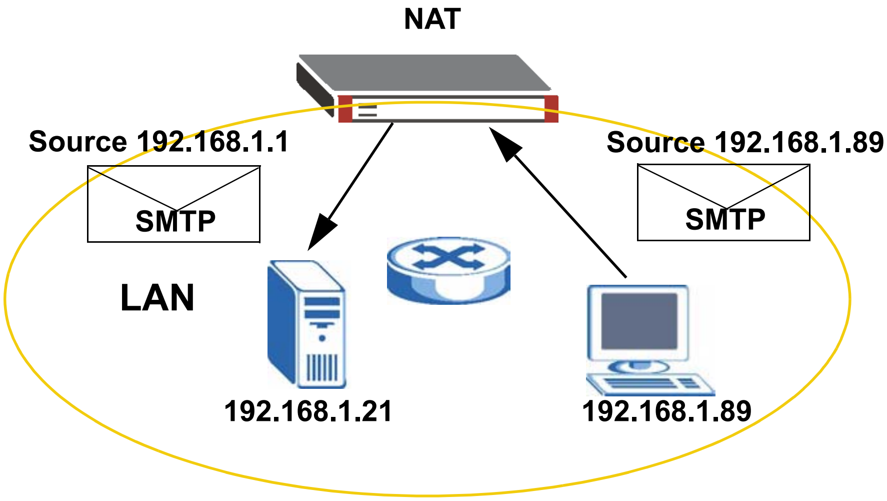
Without a NAT loopback policy route, the LAN user SMTP traffic goes to the LAN SMTP server has the LAN computer's IP address as the source. The source address is in the same subnet, so the LAN SMTP server replies directly. The return traffic uses the SMTP server's LAN IP address as the source address[1]. This creates a triangle route since the source does not match the original destination address (1.1.1.1). The user's computer shuts down the session.

Figure 100 Triangle Route



Configure a policy route to use the IP address of the ZyWALL's ge1 (LAN) interface, 192.168.1.1 as the source address of the traffic going to the LAN SMTP server from the LAN users. This way the LAN SMTP server replies to the ZyWALL and the ZyWALL applies NAT.

Figure 101 NAT Loopback Policy Route

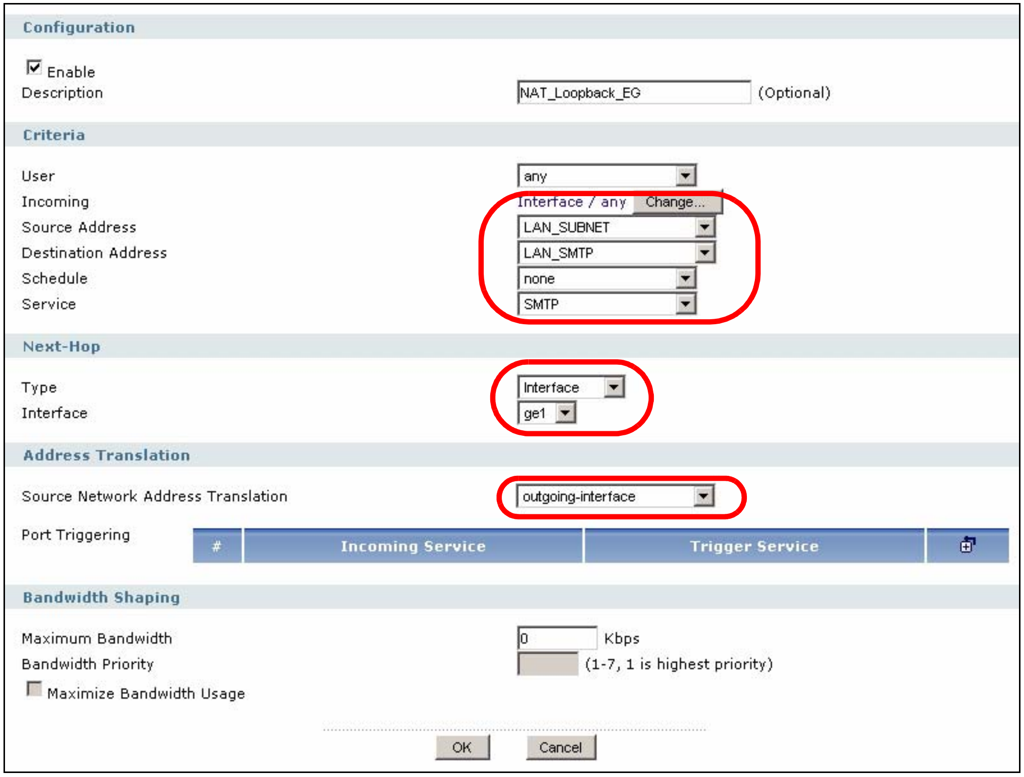


Click **Network** > **Routing** > **Policy Route** > **Add** and create the policy route as shown next. Be careful of where you create the route as routes are ordered in descending priority. This policy route applies source NAT to traffic sent from the LAN to the SMTP server.

---

[1] Even if the packets go through the ZyWALL, they only undergo layer 2 switching, not NAT.

Figure 102 Create a Policy Route



Configuration

☑ Enable

Description: NAT_Loopback_EG (Optional)

Criteria

User: any

Incoming: Interface / any Change...

Source Address: LAN_SUBNET

Destination Address: LAN_SMTP

Schedule: none

Service: SMTP

Next-Hop

Type: Interface

Interface: ge1

Address Translation

Source Network Address Translation: outgoing-interface

Port Triggering

#	Incoming Service	Trigger Service

Bandwidth Shaping

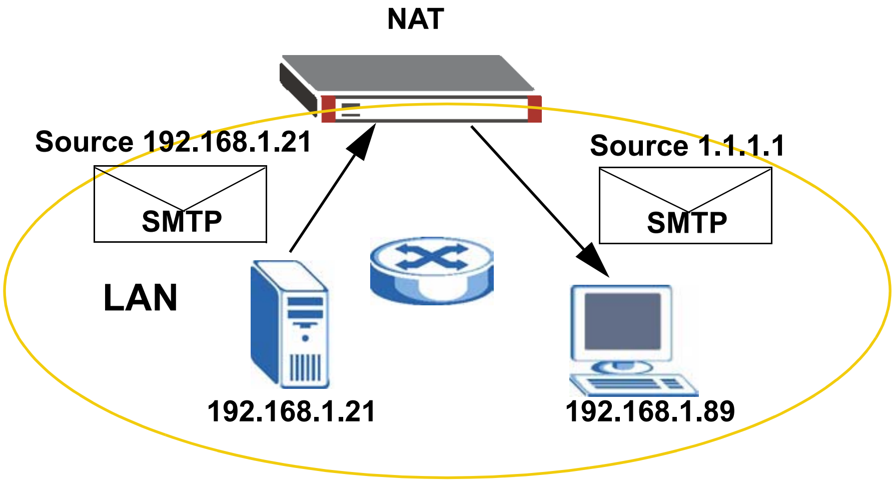
Maximum Bandwidth: 0 Kbps

Bandwidth Priority: (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

Now the LAN SMTP server replies to the ZyWALL's LAN IP address and the ZyWALL changes the source address to 1.1.1.1 before sending it to the LAN user's computer. The source in the return traffic matches the original destination address (1.1.1.1) and the LAN user can use the LAN SMTP server.

Figure 103 NAT Loopback Successful



6.8 Service Control and the Firewall

Service control lets you configure rules that control HTTP and HTTPS management access (to the web configurator) and separate rules that control HTTP and HTTPS user access (logging into SSL VPN for example). See Chapter 43 on page 575 for more on service control.

The To-ZyWALL firewall rules apply to any kind of HTTP or HTTPS connection to the ZyWALL. They do not distinguish between administrator management access and user access. If you configure service control to allow management or user HTTP or HTTPS access, make sure the firewall is not configured to block that access.

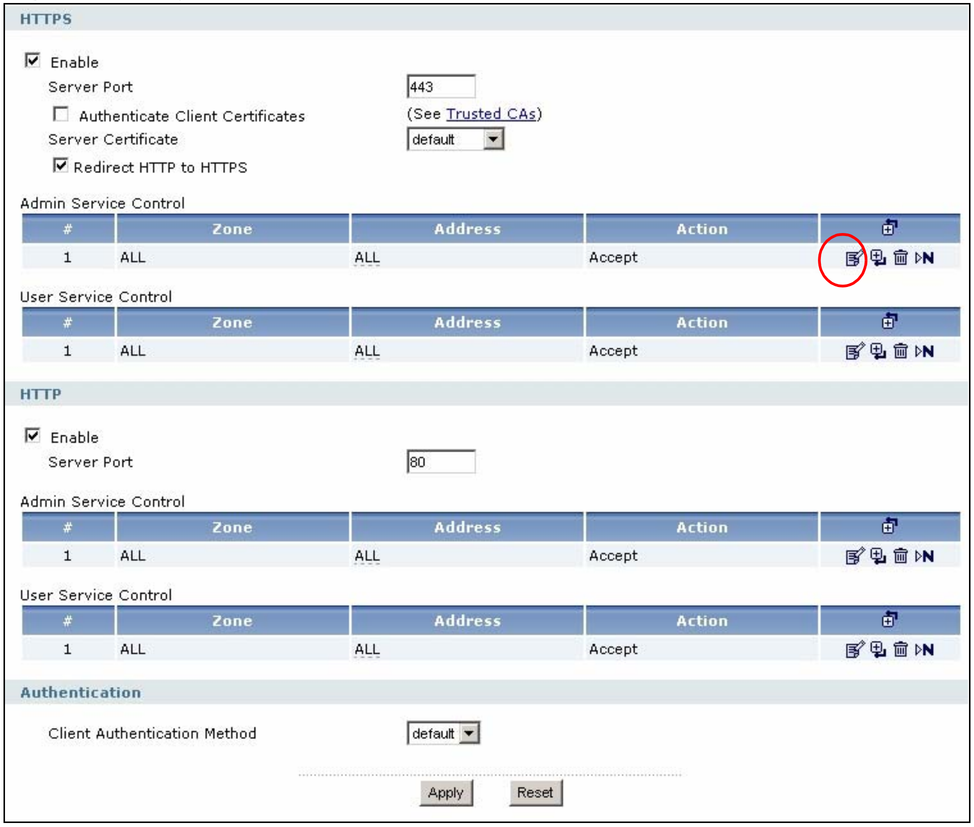
6.8.1 Allowing HTTPS Administrator Access Only From the LAN

This example configures service control to block administrator HTTPS access from all zones except the LAN.

1 Click **System** > **WWW**.

2 In HTTPS **Admin Service Control,** click the rule's **Edit** icon.

Figure 104 System > WWW



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

User Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

HTTP

☑ Enable

Server Port: 80

Admin Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

User Service Control

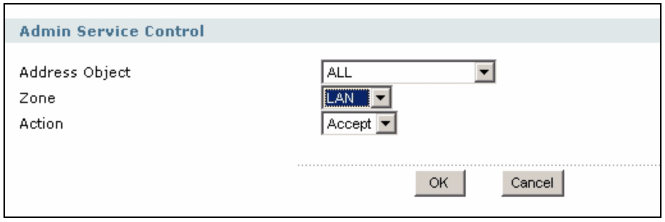
#	Zone	Address	Action
1	ALL	ALL	Accept

Authentication

Client Authentication Method: default

3 In the **Zone** field select **LAN** and click **OK**.

Figure 105 System > WWW > Service Control Rule Edit



Admin Service Control

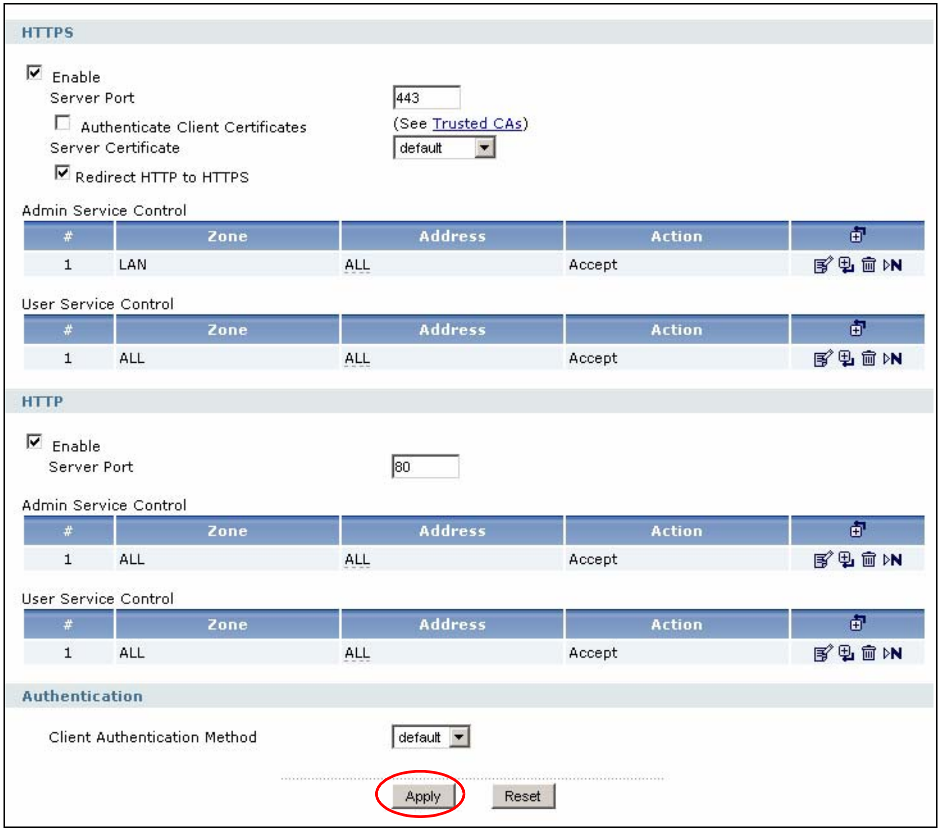
Address Object: ALL

Zone: LAN

Action: Accept

4 Click **Apply**.

Figure 106 System > WWW



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
1	LAN	ALL	Accept

User Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

HTTP

☑ Enable

Server Port: 80

Admin Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

User Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

Authentication

Client Authentication Method: default

Now administrators can only log into the web configurator from the LAN zone. Non-admin users can still use HTTPS to log into the ZyWALL from any of the ZyWALL's zones (to use SSL VPN for example).

7

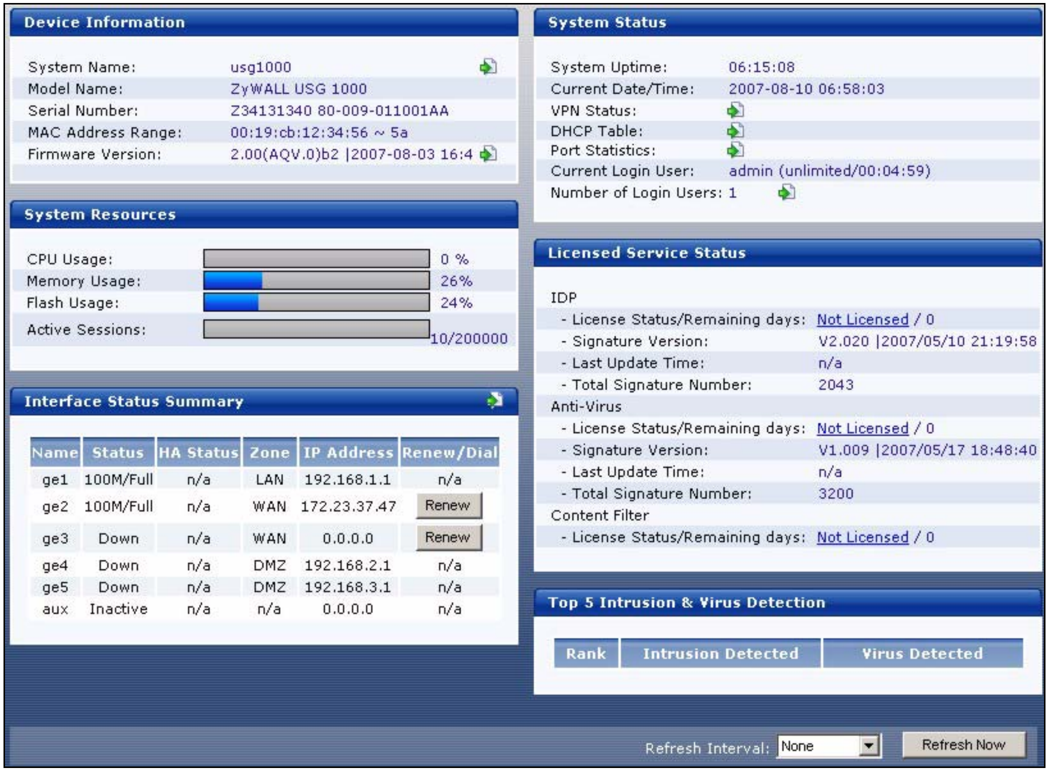
Status

This chapter explains the **Status** screen, which is the screen you see when you first log in to the ZyWALL or when you click **Status**.

7.1 Status Screen

Use this screen to look at the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status.

Figure 107 Status



Device Information

System Name: usg1000
Model Name: ZyWALL USG 1000
Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:19:cb:12:34:56 ~ 5a
Firmware Version: 2.00(AQV.0)b2 |2007-08-03 16:4

System Resources

CPU Usage: 0 %
Memory Usage: 26%
Flash Usage: 24%
Active Sessions: 10/200000

Interface Status Summary

Name	Status	HA Status	Zone	IP Address	Renew/Dial
ge1	100M/Full	n/a	LAN	192.168.1.1	n/a
ge2	100M/Full	n/a	WAN	172.23.37.47	Renew
ge3	Down	n/a	WAN	0.0.0.0	Renew
ge4	Down	n/a	DMZ	192.168.2.1	n/a
ge5	Down	n/a	DMZ	192.168.3.1	n/a
aux	Inactive	n/a	n/a	0.0.0.0	n/a

System Status

System Uptime: 06:15:08
Current Date/Time: 2007-08-10 06:58:03
VPN Status:
DHCP Table:
Port Statistics:
Current Login User: admin (unlimited/00:04:59)
Number of Login Users: 1

Licensed Service Status

IDP
- License Status/Remaining days: Not Licensed / 0
- Signature Version: V2.020 |2007/05/10 21:19:58
- Last Update Time: n/a
- Total Signature Number: 2043

Anti-Virus
- License Status/Remaining days: Not Licensed / 0
- Signature Version: V1.009 |2007/05/17 18:48:40
- Last Update Time: n/a
- Total Signature Number: 3200

Content Filter
- License Status/Remaining days: Not Licensed / 0

Top 5 Intrusion & Virus Detection

Rank	Intrusion Detected	Virus Detected

Refresh Interval: None

The following table describes the labels in this screen.

Table 34 Status

LABEL	DESCRIPTION
Device Information	
System Name	This field displays the name used to identify the ZyWALL on any network. Click the icon on the right to open the screen where you can change it. See Section 43.2 on page 575.
Model Name	This field displays the model name of this ZyWALL.
Serial Number	This field displays the serial number of this ZyWALL.
MAC Address Range	This field displays the MAC addresses used by the ZyWALL. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on.
Firmware Version	This field displays the version number and date of the firmware the ZyWALL is currently running. Click the icon on the right to open the screen where you can upload firmware. See Section 45.3 on page 620.
System Status	
System Uptime	This field displays how long the ZyWALL has been running since it last restarted or was turned on.
Current Date/ Time	This field displays the current date and time in the ZyWALL. The format is yyyy-mm-dd hh:mm:ss.
VPN Status	Click this to look at the VPN tunnels that are currently established. See Section 7.2 on page 160.
DHCP Table	Click this to look at the IP addresses currently assigned to the ZyWALL's DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 7.3 on page 161.
Port Statistics	Click this to look at packet statistics for each physical port. See Section 7.4 on page 162.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining. See Chapter 34 on page 503.
Number of Login Users	This field displays the number of users currently logged in to the ZyWALL. Click the icon to pop-open a list of the users who are currently logged in to the ZyWALL. See Section 7.5 on page 163.
System Resources	
CPU Usage	This field displays what percentage of the ZyWALL's processing capability is currently being used.
Memory Usage	This field displays what percentage of the ZyWALL's RAM is currently being used.
Flash Usage	This field displays what percentage of the ZyWALL's onboard flash memory is currently being used.
Active Sessions	This field displays how many traffic sessions are currently open on the ZyWALL. These are the sessions that are traversing the ZyWALL.
Licensed Service Status	
IDP	
License Status / Remaining Days	This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not **Licensed**, click this to open the screen where you can activate or extend the license. See Section 8.2 on page 166.

Table 34 Status (continued)

LABEL	DESCRIPTION
Signature Version	This field displays the version number, date, and time of the current set of signatures the ZyWALL is using.
Last Update Time	This field displays the last time the ZyWALL received updated signatures.
Total Signature Number	This field displays the total number of signatures in the current signature version.
Anti-Virus	
License Status / Remaining Days	This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not **Licensed**, click this to open the screen where you can activate or extend the license. See Section 8.2 on page 166.
Signature Version	This field displays the version number, date, and time of the current set of signatures the ZyWALL is using.
Last Update Time	This field displays the last time the ZyWALL received updated signatures.
Total Signature Number	This field displays the total number of signatures in the current signature version.
Content Filter	
License Status / Remaining Days	This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not **Licensed**, click this to open the screen where you can activate or extend the license. See Section 8.2 on page 166.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For port groups: **Inactive** - The port group is disabled. **Port Group Down** - The port group is enabled but not connected. **Port Group Up** - The port group is enabled, and at least one of the physical ports associated with it is connected. For Ethernet interfaces: **Port Group Inactive** - The Ethernet interface does not have any physical ports associated with it. **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For the auxiliary interface: **Inactive** - The auxiliary interface is disabled. **Connected** - The auxiliary interface is enabled and connected. **Disconnected** - The auxiliary interface is not connected.

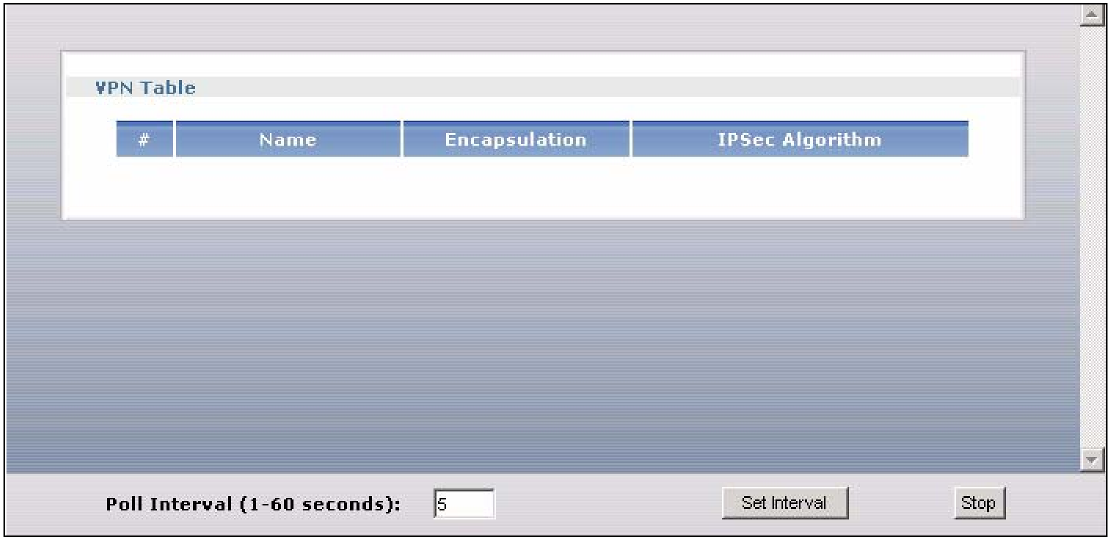
Table 34 Status (continued)

LABEL	DESCRIPTION
HA Status	This field displays the status of the interface in the virtual router. **Active** - This interface is the master interface in the virtual router. **Stand-By** - This interface is a backup interface in the virtual router. **Fault** - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down. **n/a** - Device HA is not active on the interface.
Zone	This field displays the zone to which the interface is currently assigned.
IP Address	This field displays the current IP address assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
Renew/Dial	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click the **Connect** icon to try to connect the auxiliary interface or a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.
Top 5 Intrusion & Virus Detection	The following is a list of the five intrusions or viruses that the ZyWALL has most frequently detected since it last started up.
Rank	This is the ranking number of an intrusion or virus. This is an intrusion's or virus's place in the list of most common intrusions or viruses.
Intrusion Detected	This is the name of a signature for which the ZyWALL has detected matching packets. The number in brackets indicates how many times the signature has been matched. Click the hyperlink for more detailed information on the intrusion.
Virus Detected	This is the name of the virus that the ZyWALL has detected.
Refresh Interval	Select how often you want the screen to automatically refresh.
Refresh Now	Click this to update the screen immediately.

7.2 VPN Status

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **VPN Status** in the **Status** screen.

Figure 108 Status > VPN Status



The following table describes the labels in this screen.

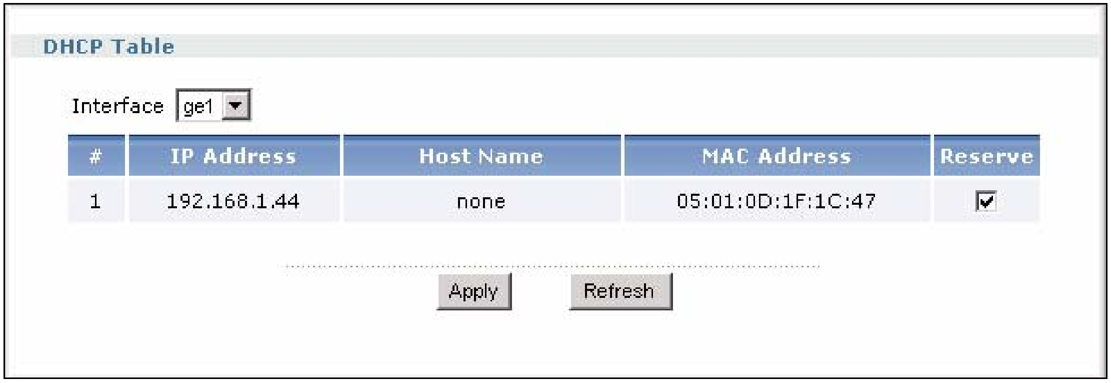
Table 35 Status > VPN Status

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
IPSec Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.

7.3 DHCP Table

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. To access this screen, click the icon beside **DHCP Table** in the **Status** screen.

Figure 109 Status > DHCP Table



Interface: ge1

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.44	none	05:01:0D:1F:1C:47	☑

The following table describes the labels in this screen.

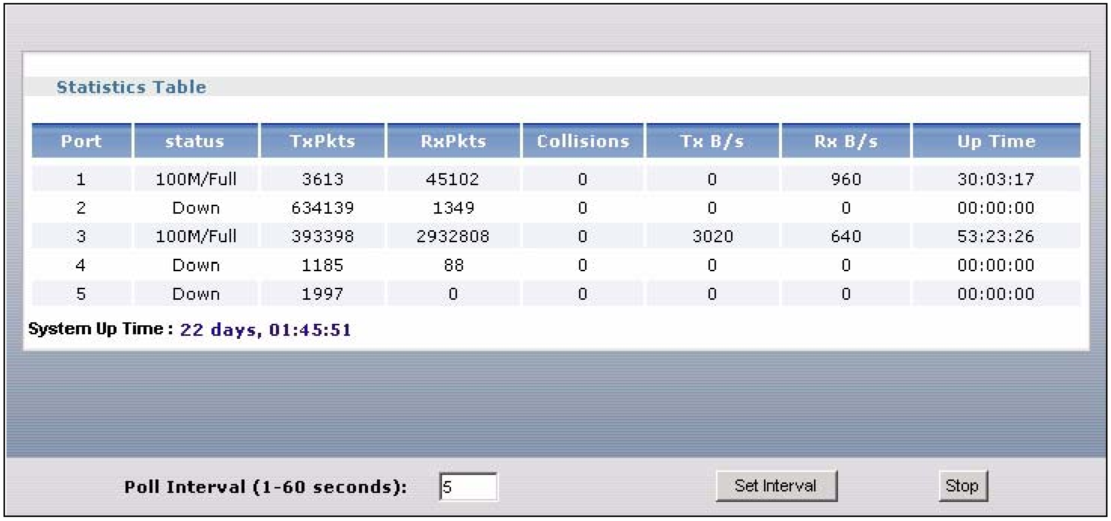
Table 36 Status > DHCP Table

LABEL	DESCRIPTION
Interface	Select for which interface you want to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address.
Host Name	This field displays the name used to identify this device on the network (the computer name). The ZyWALL learns these from the DHCP client requests. You can use CLI commands to set this value for static DHCP entries.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved.
Reserve	If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address. If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client. To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click **Apply**. To remove a static DHCP entry, clear this field, and then click **Apply**.
Apply	Click this to save your settings to the ZyWALL.
Refresh	Click this to update the screen immediately.

7.4 Port Statistics

Use this screen to look at packet statistics for each physical port. To access this screen, click **Port Statistics** in the **Status** screen.

Figure 110 Status > Port Statistics



Statistics Table

Port	status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
1	100M/Full	3613	45102	0	0	960	30:03:17
2	Down	634139	1349	0	0	0	00:00:00
3	100M/Full	393398	2932808	0	3020	640	53:23:26
4	Down	1185	88	0	0	0	00:00:00
5	Down	1997	0	0	0	0	00:00:00

System Up Time : 22 days, 01:45:51

Poll Interval (1-60 seconds): 5

The following table describes the labels in this screen.

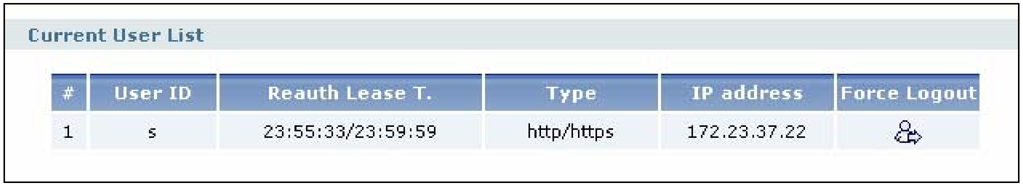
Table 37 Status > Port Statistics

LABEL	DESCRIPTION
Port	This field displays the physical port number.
status	This field displays the current status of the physical port. **Down** - The physical port is not connected. **Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the ZyWALL on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the ZyWALL on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the ZyWALL has been running since it last restarted or was turned on.
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.

7.5 Current Users

Use this screen to look at a list of the users currently logged into the ZyWALL. To access this screen, click the **Number of Login Users Detail** icon in the **Status** screen.

Figure 111 Status > Current Users



Current User List

#	User ID	Reauth Lease T.	Type	IP address	Force Logout
1	s	23:55:33/23:59:59	http/https	172.23.37.22	

The following table describes the labels in this screen.

Table 38 Status > Current Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the ZyWALL.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 34 on page 503.
Type	This field displays the way the user logged in to the ZyWALL.
IP address	This field displays the IP address of the computer used to log in to the ZyWALL.
Force Logout	Click this icon to end a user's session.

8

Registration

This chapter shows you how to register for the ZyWALL's subscription services.

8.1 myZyXEL.com Overview

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL and manage subscription services available for the ZyWALL.

You need to create an account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ZyWALL and activate a service using the **Registration** screen. Alternatively, go to http://www.myZyXEL.com with the ZyWALL's serial number and LAN MAC address to register it. Refer to the web site's online help for details.

To activate a service on a ZyWALL, you need to access myZyXEL.com via that ZyWALL.

8.1.1 Subscription Services Available on the ZyWALL

The ZyWALL can use anti-virus, IDP/AppPatrol (Intrusion Detection and Prevention and application patrol), SSL VPN, and content filtering subscription services.

- The ZyWALL's anti-virus packet scanner uses the signature files on the ZyWALL to detect virus files. After the service is activated, the ZyWALL can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).
- The IDP and application patrol features use the IDP/AppPatrol signature files on the ZyWALL. IDP detects malicious or suspicious packets and responds immediately. Application patrol conveniently manages the use of various applications on the network. After the service is activated, the ZyWALL can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).

- SSL VPN tunnels provide secure network access to remote users. You can purchase and enter a license key to have the ZyWALL use more SSL VPN tunnels.
- The content filter allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories.
- You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/AppPatrol service. You can also check for new signatures at http://mysecurity.zyxel.com.

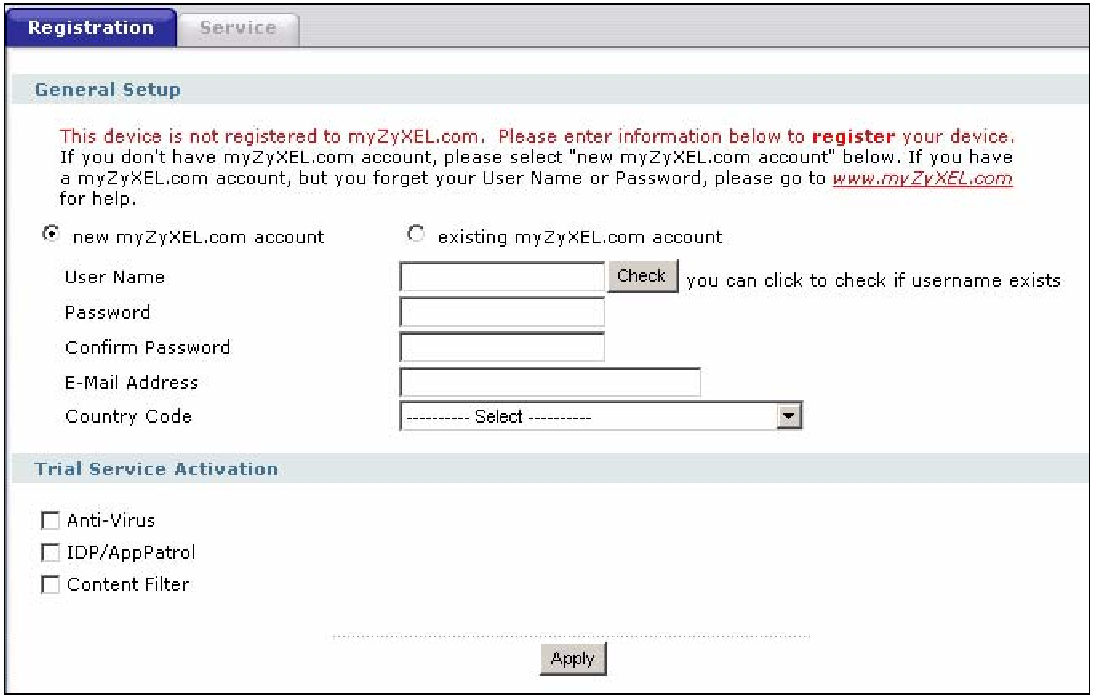
See the respective chapters for more information about these features.

To update the signature file or use a subscription service, you have to register the ZyWALL and activate the corresponding service at myZyXEL.com (through the ZyWALL).

8.2 Registration

Use this screen to register your ZyWALL with myZyXEL.com and activate a service, such as content filtering. Click **Licensing > Registration** in the navigation panel to open the screen as shown next.

Figure 112 Licensing > Registration



General Setup

This device is not registered to myZyXEL.com. Please enter information below to **register** your device. If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have a myZyXEL.com account, but you forget your User Name or Password, please go to www.myZyXEL.com for help.

● new myZyXEL.com account ○ existing myZyXEL.com account

User Name

you can click to check if username exists

Password

Confirm Password

E-Mail Address

Country Code ---------- Select ----------

Trial Service Activation

☐ Anti-Virus
☐ IDP/AppPatrol
☐ Content Filter

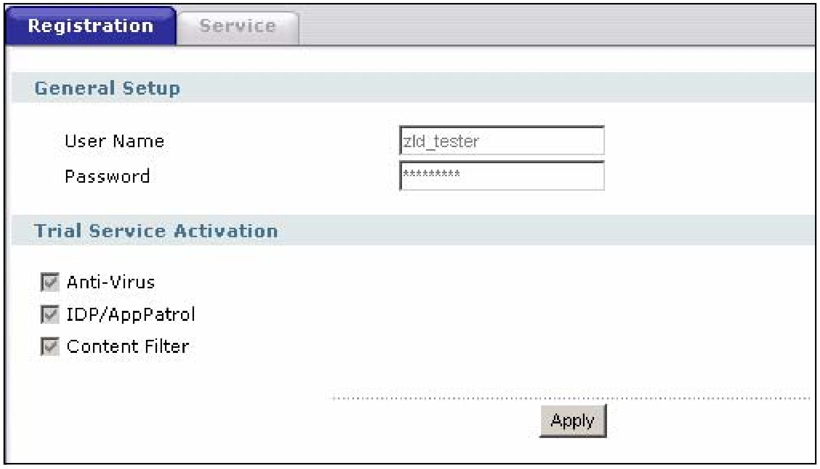
The following table describes the labels in this screen.

Table 39 Licensing > Registration

LABEL	DESCRIPTION
General Setup	If you select **existing myZyXEL.com account**, only the **User Name** and **Password** fields are available.
new myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL.
existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL.
UserName	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country Code	Select your country from the drop-down box list.
Trial Service Activation	You can try a trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the **Registration Service** screen to extend the service.
Anti-Virus IDP/AppPatrol Content Filter	Select the check box to activate a trial. The trial period starts the day you activate the trial.
Apply	Click **Apply** to save your changes back to the ZyWALL.

If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Service** screen to update your service subscription status.

Figure 113 Licensing > Registration: Registered Device


Registration
Service
General Setup

User Name: zld_tester

Password: *********

Trial Service Activation

☑ Anti-Virus

☑ IDP/AppPatrol

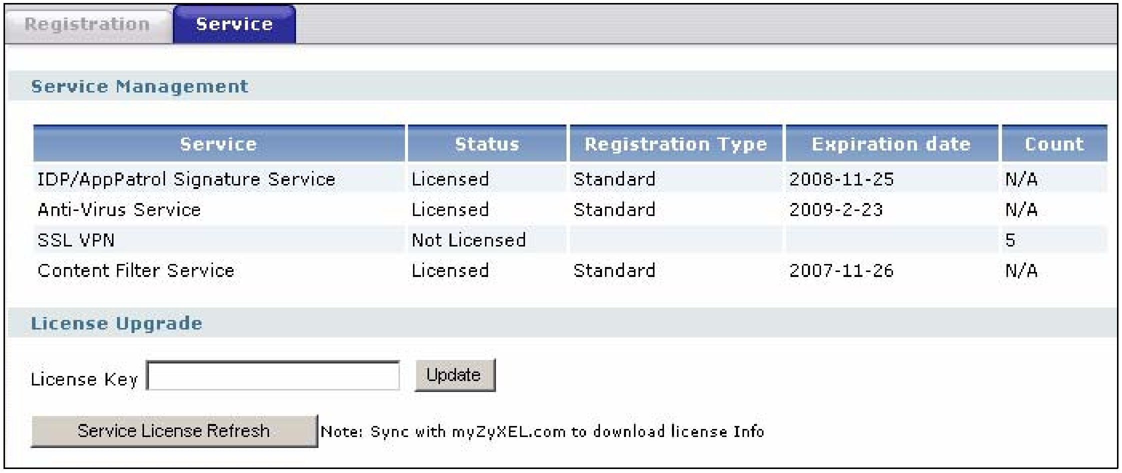
☑ Content Filter

Apply

8.3 Service

After you activate a trial, you can also use this screen to register and enter your iCard's PIN number (license key). Click **Licensing** > **Registration** > **Service** to open the screen as shown next.

Figure 114 Licensing > Registration > Service


Registration
Service
Service Management

Service	Status	Registration Type	Expiration date	Count
IDP/AppPatrol Signature Service	Licensed	Standard	2008-11-25	N/A
Anti-Virus Service	Licensed	Standard	2009-2-23	N/A
SSL VPN	Not Licensed			5
Content Filter Service	Licensed	Standard	2007-11-26	N/A

License Upgrade
License Key
Update
Service License Refresh

Note: Sync with myZyXEL.com to download license Info

The following table describes the labels in this screen.

Table 40 Licensing > Registration > Service

LABEL	DESCRIPTION
Service Management	
Service	This field displays the service name available on the ZyWALL.
Status	This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**).
Registration Type	This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). This field is blank when a service is not activated.

Table 40 Licensing > Registration > Service (continued)

LABEL	DESCRIPTION
Expiration date	This field displays the date your service expires. You can continue to use IDP/AppPatrol or Anti-Virus after the registration expires, you just won't receive updated signatures.
Count	This field displays how many VPN tunnels you can use with your current license. This field does not apply to the other services.
License Upgrade	
License Key	Enter your iCard's PIN number and click **Update** to activate or extend a standard service subscription. If a standard service subscription runs out, you need to buy a new iCard (specific to your ZyWALL) and enter the new PIN number to extend the service.
Service License Refresh	Click this button to renew service license information (such as the registration status and expiration day).

9

Update

This chapter shows you how to update the ZyWALL's signature packages.

9.1 Updating Anti-virus Signatures

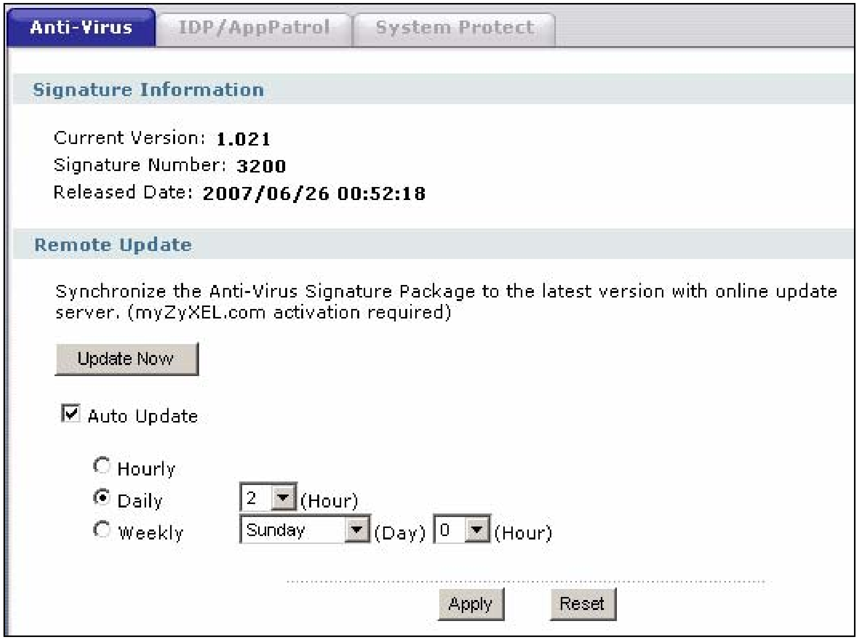
When scheduling signature updates, choose a day and time when your network is least busy to minimize disruption to your network. Your custom signature configurations are not overwritten when you download new signatures.

IDP signatures (see the chapters on IDP) are included with string-based anti-virus signatures. When you download new signatures using the IDP **Update** screen, anti-virus signatures are also downloaded. The version number changes both in the IDP **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

The ZyWALL does not have to reboot when you upload new signatures.

Click **Licensing > Update >Anti-Virus** to display the following screen.

Figure 115 Licensing > Update >Anti-Virus



Current Version: 1.021
Signature Number: 3200
Released Date: 2007/06/26 00:52:18

Synchronize the Anti-Virus Signature Package to the latest version with online update server. (myZyXEL.com activation required)

☑ Auto Update

○ Hourly
● Daily 2 (Hour)
○ Weekly Sunday (Day) 0 (Hour)

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Signature Information	
Current Version	This field displays the signatures version number currently used by the ZyWALL. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them. This number gets larger as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications.
Signature Number	This field displays the number of signatures in this set.
Released Date	This field displays the date and time the set was released.
Remote Update	Use these fields to have the ZyWALL check for new signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL.
Update Now	Click this button to have the ZyWALL check for new signatures immediately. If there are new ones, the ZyWALL will then download them.
Auto Update	Select this check box to have the ZyWALL automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Hourly	Select this option to have the ZyWALL check for new signatures every hour.
Daily	Select this option to have the ZyWALL check for new signatures every day at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example.
Weekly	Select this option to have the ZyWALL check for new signatures once a week on the day and at the time specified.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

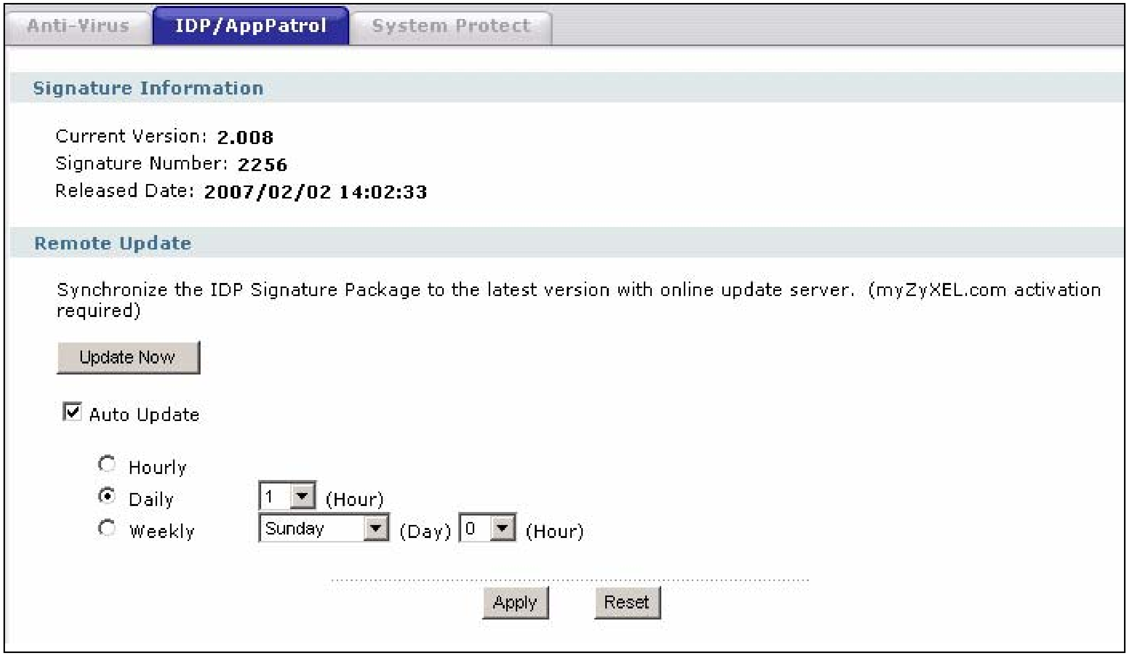
9.2 Updating IDP and Application Patrol Signatures

The ZyWALL comes with signatures for the IDP and application patrol features. These signatures are continually updated as new attack types evolve. New signatures can be downloaded to the ZyWALL periodically if you have subscribed for IDP service.

You need to create an account at myZyXEL.com, register your ZyWALL and then subscribe for IDP service in order to be able to download new packet inspection signatures from myZyXEL.com (see the **Registration** screens). Use the **Update IDP /AppPatrol** screen to schedule or immediately download IDP signatures.

Click **Licensing > Update > IDP/AppPatrol** to display the following screen.

Figure 116 Licensing > Update > IDP/AppPatrol



Current Version: 2.008
Signature Number: 2256
Released Date: 2007/02/02 14:02:33

Synchronize the IDP Signature Package to the latest version with online update server. (myZyXEL.com activation required)

☑ Auto Update

○ Hourly
● Daily 1 (Hour)
○ Weekly Sunday (Day) 0 (Hour)

The following table describes the fields in this screen.

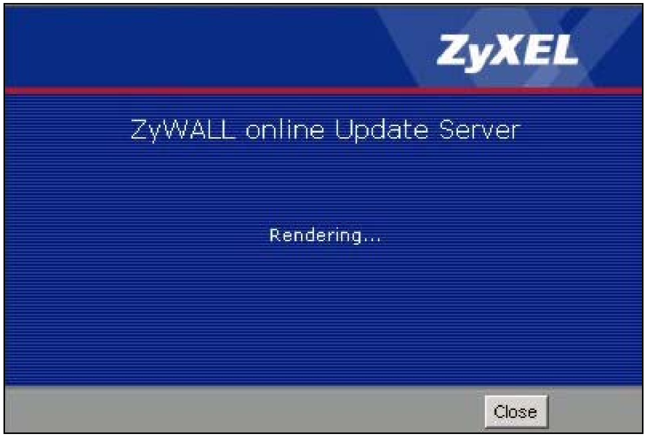
Table 41 Licensing > Update > IDP/AppPatrol

LABEL	DESCRIPTION
Signature Information	The following fields display information on the current signature set that the ZyWALL is using.
Current Version	This field displays the IDP signature and anomaly rule set version number. This number gets larger as the set is enhanced.
Signature Number	This field displays the number of IDP signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones.
Released Date	This field displays the date and time the set was released.
Remote Update	Use these fields to have the ZyWALL check for new IDP signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL.
Update Now	Click this button to have the ZyWALL check for new IDP signatures immediately. If there are new ones, the ZyWALL will then download them.

Table 41 Licensing > Update > IDP/AppPatrol (continued)

LABEL	DESCRIPTION
Auto Update	Select this check box to have the ZyWALL automatically check for new IDP signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Hourly	Select this option to have the ZyWALL check for new IDP signatures every hour.
Daily	Select this option to have the ZyWALL check for new IDP signatures everyday at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example.
Weekly	Select this option to have the ZyWALL check for new IDP signatures once a week on the day and at the time specified.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

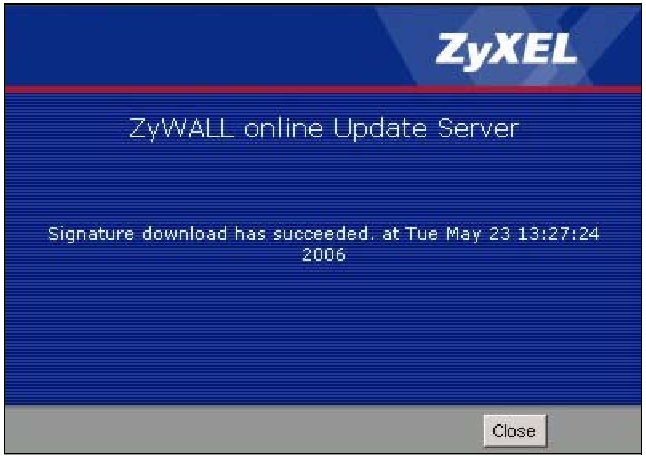
Figure 117 Downloading IDP Signatures



ZyWALL online Update Server

Rendering...

Figure 118 Successful IDP Signature Download



ZyWALL online Update Server

Signature download has succeeded. at Tue May 23 13:27:24 2006

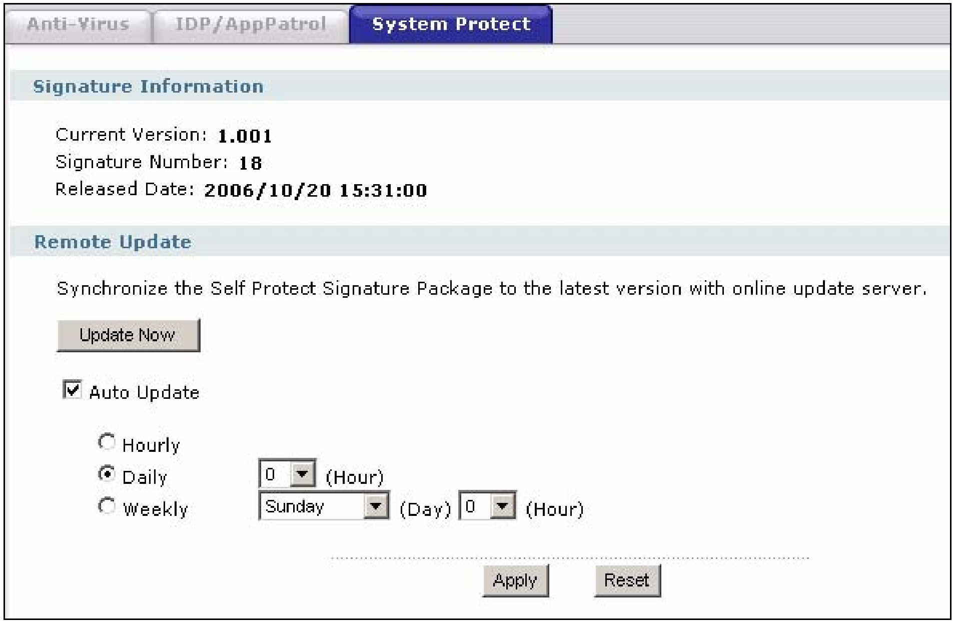
9.3 Updating System Protect Signatures

The ZyWALL comes with signatures that the ZyWALL uses to protect itself from intrusions. These signatures are continually updated as new attack types evolve. These system protect signature updates are free and can be downloaded to the ZyWALL periodically.

Click **Licensing** > **Update** > **System Protect** to display the following screen.

Use this screen to schedule or immediately download IDP signatures.

Figure 119 Licensing > Update > System Protect



Current Version: 1.001
Signature Number: 18
Released Date: 2006/10/20 15:31:00

Synchronize the Self Protect Signature Package to the latest version with online update server.

☑ Auto Update

○ Hourly
● Daily 0 (Hour)
○ Weekly Sunday (Day) 0 (Hour)

The following table describes the fields in this screen.

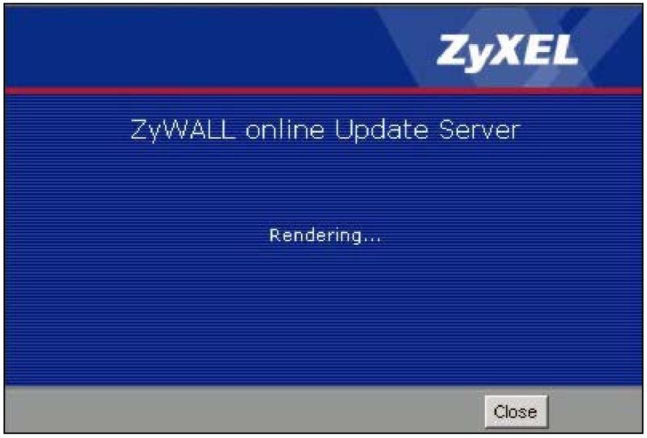
Table 42 Licensing > Update > System Protect

LABEL	DESCRIPTION
Signature Information	The following fields display information on the current signature set that the ZyWALL is using.
Current Version	This field displays the IDP signature and anomaly rule set version number. This number gets larger as the set is enhanced.
Signature Number	This field displays the number of signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones.
Released Date	This field displays the date and time the set was released.
Remote Update	Use these fields to have the ZyWALL check for new signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL.
Update Now	Click this button to have the ZyWALL check for new signatures immediately. If there are new ones, the ZyWALL will then download them.
Auto Update	Select this check box to have the ZyWALL automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Hourly	Select this option to have the ZyWALL check for new signatures every hour.

Table 42 Licensing > Update > System Protect (continued)

LABEL	DESCRIPTION
Daily	Select this option to have the ZyWALL check for new signatures every day at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example.
Weekly	Select this option to have the ZyWALL check for new signatures once a week on the day and at the time specified.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

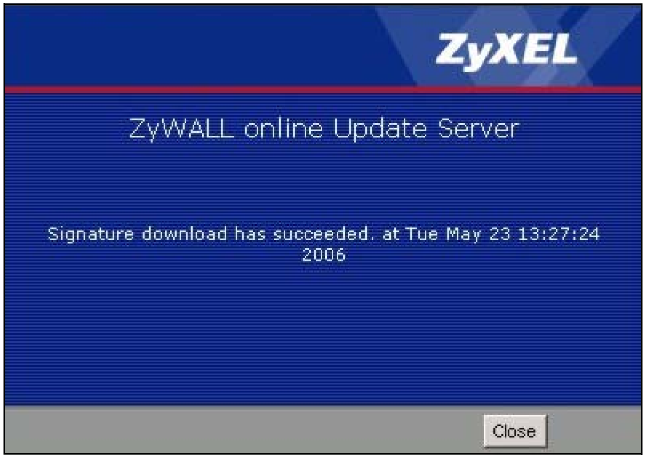
Figure 120 Downloading System Protect Signatures



ZyWALL online Update Server

Rendering...

Figure 121 Successful System Protect Signature Download



ZyWALL online Update Server

Signature download has succeeded. at Tue May 23 13:27:24 2006

PART II

Network

Interface (179)
Trunks (219)
Policy and Static Routes (225)
Routing Protocols (235)
Zones (245)
DDNS (249)
Virtual Servers (255)
HTTP Redirect (261)
ALG (265)

10

Interface

See Section 5.4.2 on page 115 for related information on these screens.

10.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interface can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

10.1.1 Types of Interfaces

You can create several types of interfaces in the ZyWALL.

- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** provide additional routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **AUX**port.

- **Trunks** manage load balancing between interfaces.

Port groups, trunks, and the auxiliary interface have a lot of characteristics that are specific to each type of interface. They are discussed in more detail in Section 10.3.1 on page 194, Chapter 11 on page 219, and Section 10.7.1 on page 215, respectively. The other types of interfaces--Ethernet, VLAN, bridge, PPPoE/PPTP, and virtual--have a lot of similar characteristics. These characteristics are listed in the following table and discussed in more detail below.

Table 43 Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interfaces Characteristics

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE/PPTP	VIRTUAL
Name*	ge*x*	vlan*x*	br*x*	ppp*x*	**
IP Address Assignment					
static IP address	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	Yes	Yes	Yes	No
routing metric	Yes	Yes	Yes	Yes	Yes
Interface Parameters					
bandwidth restrictions	Yes	Yes	Yes	Yes	Yes
packet size (MTU)	Yes	Yes	Yes	Yes	No
DHCP					
DHCP server	Yes	Yes	Yes	No	No
DHCP relay	Yes	Yes	Yes	No	No
Ping Check	Yes	Yes	Yes	Yes	No

* - The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*, limited by the maximum number of each type of interface). For example, Ethernet interface names are ge1, ge2, ge3, ...; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface ge1 are called ge1:1, ge1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

10.1.2 IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

Figure 122 Example: Entry in the Routing Table Derived from Interfaces

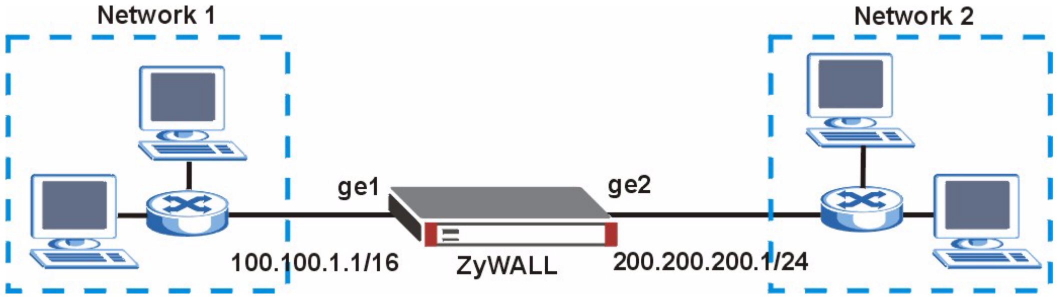


Table 44 Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	ge1
200.200.200.1/24	ge2

For example, if the ZyWALL gets a packet with a destination address of 100.100.25.25, it routes the packet to interface ge1. If the ZyWALL gets a packet with a destination address of 200.200.200.200, it routes the packet to interface ge2.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the ZyWALL gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the ZyWALL should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on ge2. In this case, the ZyWALL creates the following entry in the routing table.

Table 45 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the ZyWALL uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the ZyWALL uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

10.1.3 Interface Parameters

The ZyWALL restricts the amount of traffic into and out of the ZyWALL through each interface.

- Upstream bandwidth is the amount of traffic from the ZyWALL through the interface to the network.
- Downstream bandwidth is the amount of traffic from the network through the interface into the ZyWALL.[2]

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The ZyWALL also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the ZyWALL divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

10.1.4 DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

In the ZyWALL, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the ZyWALL's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

Table 46 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200

---

[2] At the time of writing, the ZyWALL does not support downstream bandwidth management.

Table 46 Example: Assigning IP Addresses from a Pool (continued)

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

The ZyWALL cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the ZyWALL cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the ZyWALL cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See Section 10.1.2 on page 180.
- Gateway - The interface provides the same gateway you specify for the interface. See Section 10.1.2 on page 180.
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

10.1.4.1 WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

10.1.5 Ping Check Settings

The interface can regularly ping the gateway you specified (see Section 10.1.2 on page 180) to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.

10.1.6 Relationships Between Interfaces

In the ZyWALL, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

Table 47 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
auxiliary interface	auxiliary port
port group	physical port
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPPoE/PPTP interface	Ethernet interface* VLAN interface* bridge interface
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface VLAN interface bridge interface PPPoE/PPTP interface auxiliary interface

* - You cannot set up a PPPoE/PPTP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPPoE/PPTP interface on top of it.

10.2 Ethernet Interfaces

This section introduces Ethernet interfaces and then explains the screens for Ethernet interfaces.

10.2.1 Ethernet Interfaces Overview

The ZyWALL has five Ethernet interfaces: ge1, ge2, ge3, ge4, and ge5. Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of these five. If you do not assign any physical ports to an Ethernet interface (see Section 10.3.1 on page 194), the Ethernet interface is effectively removed from the ZyWALL, but you can still configure it.

Ethernet interfaces are similar to other types of interfaces in many other ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict the amount of bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

In addition, you use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management.

The ZyWALL supports two routing protocols, RIP and OSPF. See Chapter 13 on page 235 for background information about these routing protocols.

With RIP, you can use Ethernet interfaces to do the following things.

- Enable and disable RIP in the underlying physical port or port group.
- Select which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Select which version of RIP to support in each direction - The ZyWALL supports RIP-1, RIP-2, and both versions.
- Select the broadcasting method used by RIP-2 packets - The ZyWALL can use subnet broadcasting or multicasting.

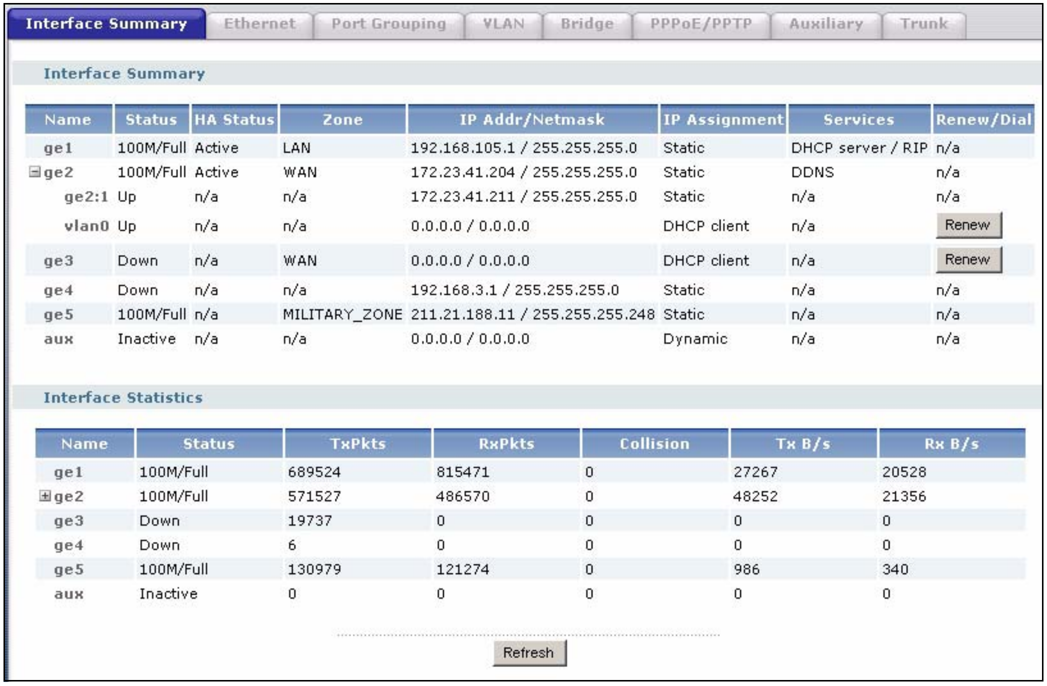
With OSPF, you can use Ethernet interfaces to do the following things.

- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Set the priority used to identify the DR or BDR if one does not exist.

10.2.2 Interface Summary Screen

This screen lists all of the ZyWALL’s interfaces and gives packet statistics for them. Click **Network** > **Interface** to access this screen.

Figure 123 Network > Interface > Interface Summary



Interface Summary

Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial
ge1	100M/Full	Active	LAN	192.168.105.1 / 255.255.255.0	Static	DHCP server / RIP	n/a
⊟ge2	100M/Full	Active	WAN	172.23.41.204 / 255.255.255.0	Static	DDNS	n/a
ge2:1	Up	n/a	n/a	172.23.41.211 / 255.255.255.0	Static	n/a	n/a
vlan0	Up	n/a	n/a	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
ge3	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
ge4	Down	n/a	n/a	192.168.3.1 / 255.255.255.0	Static	n/a	n/a
ge5	100M/Full	n/a	MILITARY_ZONE	211.21.188.11 / 255.255.255.248	Static	n/a	n/a
aux	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a

Interface Statistics

Name	Status	TxPkts	RxPkts	Collision	Tx B/s	Rx B/s
ge1	100M/Full	689524	815471	0	27267	20528
⊞ge2	100M/Full	571527	486570	0	48252	21356
ge3	Down	19737	0	0	0	0
ge4	Down	6	0	0	0	0
ge5	100M/Full	130979	121274	0	986	340
aux	Inactive	0	0	0	0	0

Each field is described in the following table.

Table 48 Network > Interface > Interface Summary

LABEL	DESCRIPTION
Interface Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Name	This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface.

Table 48 Network > Interface > Interface Summary (continued)

LABEL	DESCRIPTION
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For port groups: **Inactive** - The port group is disabled. **Port Group Down** - The port group is enabled but not connected. **Port Group Up** - The port group is enabled, and at least one of the physical ports associated with it is connected. For Ethernet interfaces: **Port Group Inactive** - The Ethernet interface does not have any physical ports associated with it. **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For the auxiliary interface: **Inactive** - The auxiliary interface is disabled. **Connected** - The auxiliary interface is enabled and connected. **Disconnected** - The auxiliary interface is not connected. For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPPoE/PPTP interfaces: **Connected** - The PPPoE/PPTP interface is connected. **Disconnected** - The PPPoE/PPTP interface is not connected. If the PPPoE/PPTP interface is disabled, it does not appear in the list.
HA Status	This field displays the status of the interface in the virtual router. **Active** - This interface is the master interface in the virtual router. **Stand-By** - This interface is a backup interface in the virtual router. **Fault** - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down. **n/a** - Device HA is not active on the interface.
Zone	This field displays the zone to which the interface is currently assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server. **Dynamic** - This is the auxiliary interface.
Services	This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. This field displays **n/a** if the interface does not provide any services to the network.
Renew/Dial	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click the **Connect** icon to try to connect the auxiliary interface or a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.

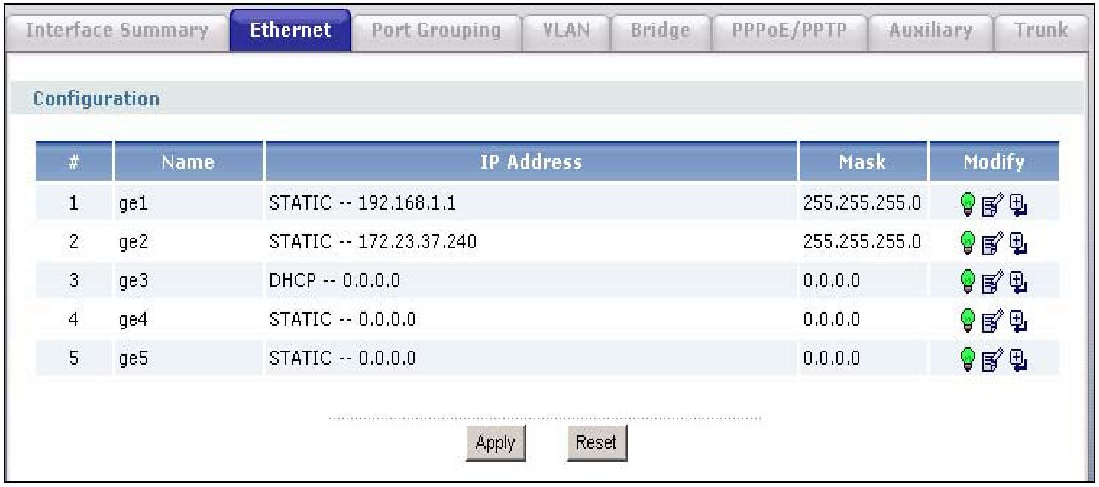
Table 48 Network > Interface > Interface Summary (continued)

LABEL	DESCRIPTION
Interface Statistics	This table provides packet statistics for each interface.
Name	This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the statistics for virtual interfaces on top of this interface.
Status	This field displays the current status of the interface. **Down** - The interface is not connected. **Speed / Duplex** - The interface is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the ZyWALL on the interface since it was last connected.
RxPkts	This field displays the number of packets received by the ZyWALL on the interface since it was last connected.
Collision	This field displays the number of collisions on the interface since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated.
Refresh	Click this button to update the information in the screen.

10.2.3 Ethernet Summary Screen

This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. To access this screen, click **Network** > **Interface**.

Figure 124 Network > Interface > Ethernet



#	Name	IP Address	Mask	Modify
1	ge1	STATIC -- 192.168.1.1	255.255.255.0	
2	ge2	STATIC -- 172.23.37.240	255.255.255.0	
3	ge3	DHCP -- 0.0.0.0	0.0.0.0	
4	ge4	STATIC -- 0.0.0.0	0.0.0.0	
5	ge5	STATIC -- 0.0.0.0	0.0.0.0	

Each field is described in the following table.

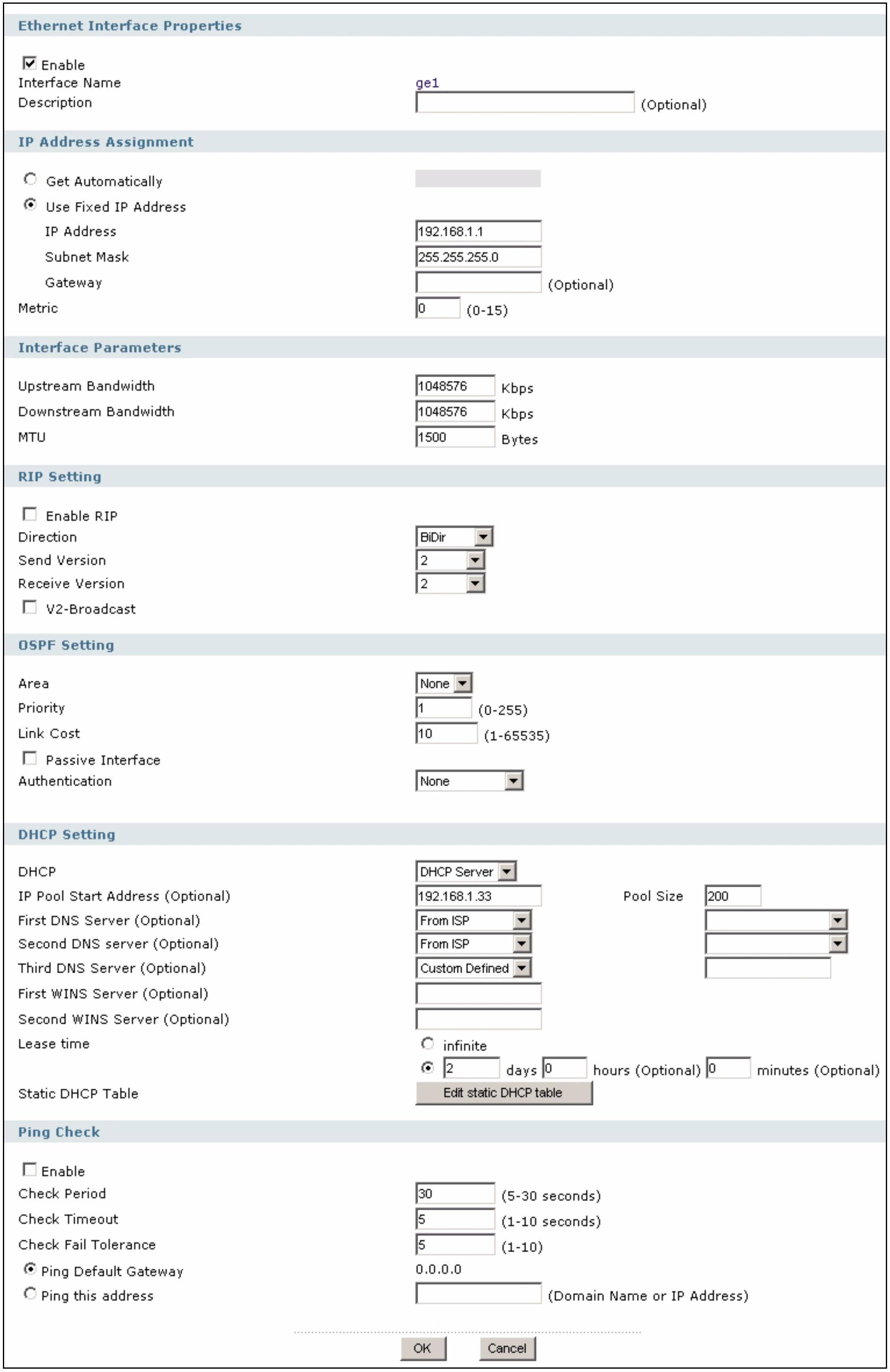
Table 49 Network > Interface > Ethernet

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Modify	This column lets you create, edit, remove, activate, and deactivate interfaces. You cannot add or remove Ethernet interfaces, however. To create a virtual Ethernet interface, click the **Add** icon next to the corresponding Ethernet interface. The **Virtual Interface Add/Edit** screen appears. See Section 10.8 on page 217. To edit an interface, click the **Edit** icon next to it. The **Ethernet Edit** screen or **Virtual Interface Add/Edit** screen appears accordingly. To remove a virtual interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

10.2.4 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, and ping check settings. To access this screen, click an **Edit** icon in the **Ethernet Summary** screen. (See Section 10.2.3 on page 188.)

Figure 125 Network > Interface > Ethernet > Edit



Ethernet Interface Properties

☑ Enable
Interface Name: ge1
Description: (Optional)

IP Address Assignment

○ Get Automatically
● Use Fixed IP Address
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: (Optional)
Metric: 0 (0-15)

Interface Parameters

Upstream Bandwidth: 1048576 Kbps
Downstream Bandwidth: 1048576 Kbps
MTU: 1500 Bytes

RIP Setting

☐ Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
☐ V2-Broadcast

OSPF Setting

Area: None
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
☐ Passive Interface
Authentication: None

DHCP Setting

DHCP: DHCP Server
IP Pool Start Address (Optional): 192.168.1.33 Pool Size: 200
First DNS Server (Optional): From ISP
Second DNS server (Optional): From ISP
Third DNS Server (Optional): Custom Defined
First WINS Server (Optional):
Second WINS Server (Optional):
Lease time: ○ infinite
● 2 days 0 hours (Optional) 0 minutes (Optional)
Static DHCP Table: Edit static DHCP table

Ping Check

☐ Enable
Check Period: 30 (5-30 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
● Ping Default Gateway: 0.0.0.0
○ Ping this address: (Domain Name or IP Address)

Each field is described in the table below.

Table 50 Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
Ethernet Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Name	This field is read-only. This is the name of the Ethernet interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	These IP address fields configure an IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group. See Chapter 33 on page 493.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
RIP Settings	See Section 13.1.1 on page 235 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.

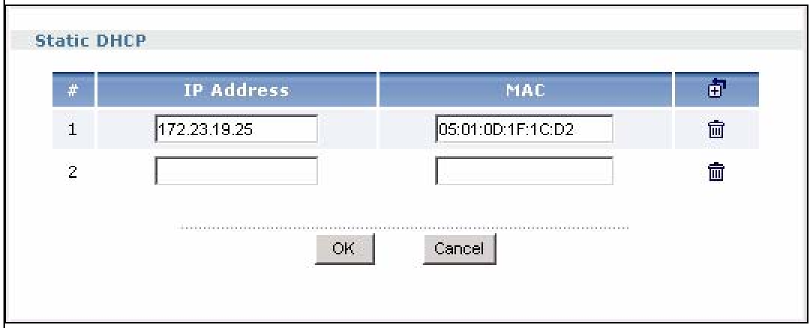
Table 50 Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ZyWALL uses multicasting.
OSPF Setting	See Section 13.3 on page 237 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to eight characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
DHCP Settings	
DHCP	Select what type of DHCP service the ZyWALL provides to the network. Choices are: **None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.

Table 50 Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. The ZyWALL provides these IP addresses to DHCP clients. You can specify these IP addresses two ways. **Custom Defined** - enter a static IP address. **From ISP** - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire. **days, hours, and minutes** - select this to enter how long IP addresses are valid.

Table 50 Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Edit static DHCP table	Click this if you want the ZyWALL to assign static IP addresses to computers. The **Static DHCP** screen appears. **Figure 126** Network > Interface > Ethernet > Edit > Edit static DHCP table  1 172.23.19.25 05:01:0D:1F:1C:D2 2 The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns the IP address dynamically using the **IP Pool Start Address** and **Pool Size**. Note: You must click **OK** in the **Static DHCP** screen and then click **OK** in this screen to save your changes.
Ping Check	The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.
Enable	Select this to enable the ping check.
Check Period	Enter the number of seconds between ping attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Ping Default Gateway	Select this to ping the default gateway.
Ping this address	Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.

10.3 Port Grouping

This section introduces port groups and then explains the screen for port groups.

10.3.1 Port Grouping Overview

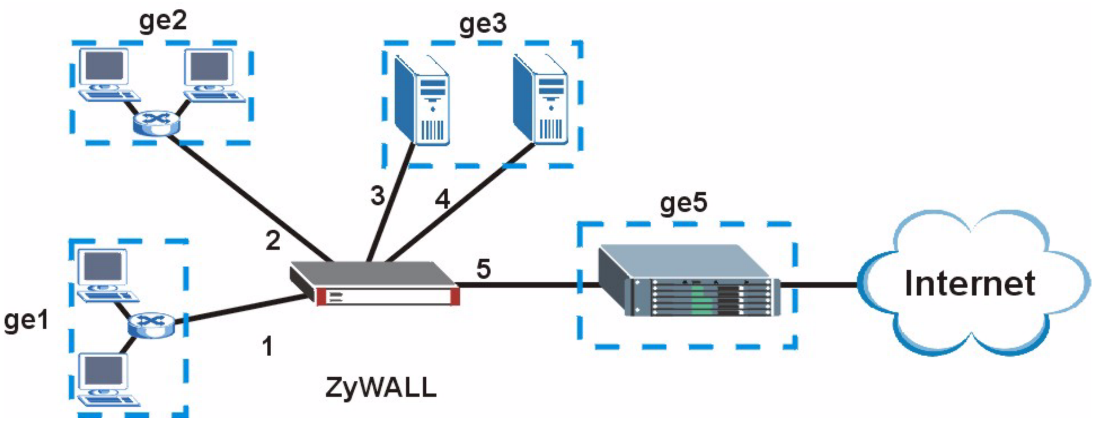
Use port grouping to create port groups and to assign physical ports and port groups to Ethernet interfaces.

Each physical port is assigned to one Ethernet interface. In port grouping, the Ethernet interfaces are called **representative interfaces**. If you assign more than one physical port to a representative interface, you create a **port group**. Port groups have the following characteristics:

- There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security.
- It can increase the bandwidth between the port group and other interfaces.

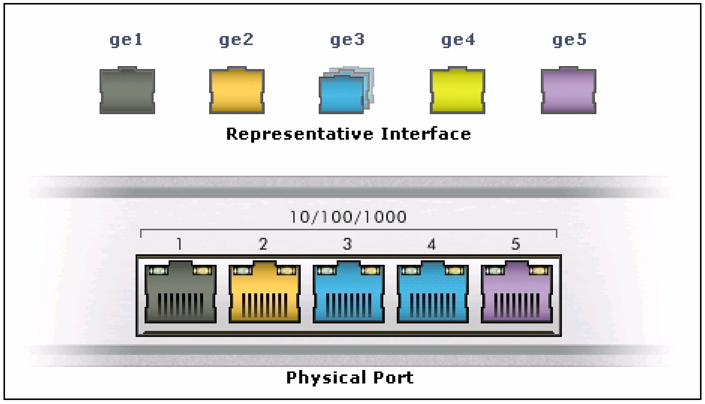
In the example below, you might combine physical ports 3 and 4 into port group ge3.

Figure 127 Port Grouping Example: Network



In this case, click **Network > Interface > Port Grouping**, and set up the screen like this.

Figure 128 Port Grouping Example: Screen

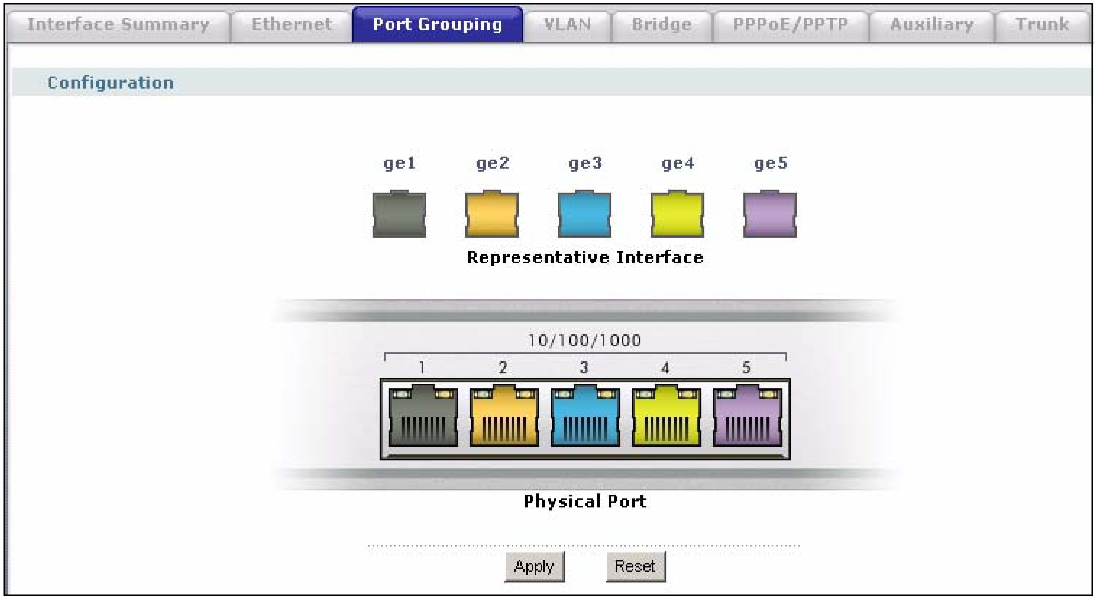


There are no ports assigned to ge4. If you do not assign any physical ports to a representative interface, you cannot use this interface to create other interfaces or create IPSec VPN tunnels. The Ethernet interface is still displayed in the screen, however, and the existing configuration remains.

10.3.2 Port Grouping Screen

You can maintain the relationship between physical ports, port groups, and Ethernet interfaces in the **Port Grouping** screen. To access this screen, click **Network** > **Interface** > **Port Grouping**.

Figure 129 Network > Interface > Port Grouping


Interface Summary
Ethernet
Port Grouping
VLAN
Bridge
PPPoE/PPTP
Auxiliary
Trunk
Configuration
ge1
ge2
ge3
ge4
ge5
Representative Interface
10/100/1000
1
2
3
4
5
Physical Port
Apply
Reset

Each section in this screen is described below.

Table 51 Network > Interface > Port Grouping

LABEL	DESCRIPTION
Representative Interface (ge1, ge2, ge3, ge4, ge5)	These are Ethernet interfaces. To add a physical port to a representative interface, drag the physical port onto the corresponding representative interface.
Physical Port (1, 2, 3, 4, 5)	These are the physical ports as they appear on the front panel of the ZyWALL. To add a physical port to a representative interface, drag the physical port onto the corresponding representative interface.
Apply	Click this button to save your changes and apply them to the ZyWALL.
Reset	Click this button to change the port groups to their current configuration (last-saved values).

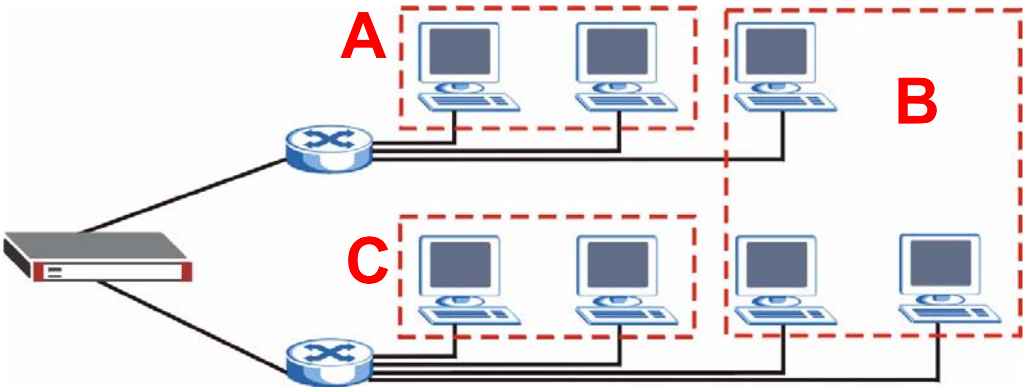
10.4 VLAN Interfaces

This section introduces VLAN and VLAN interfaces and then explains the screens for VLAN interfaces.

10.4.1 VLAN Overview

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

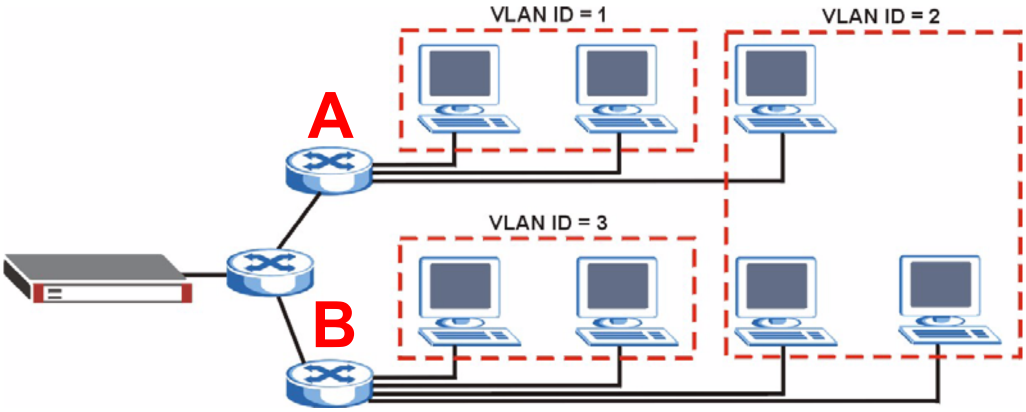
Figure 130 Example: Before VLAN



In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Alternatively, you can divide the physical networks into three VLANs.

Figure 131 Example: After VLAN



Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.

- Better manageability - You can align network policies more appropriately for users. For example, you can create different content filtering rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

10.4.2 VLAN Interfaces Overview

In the ZyWALL, each VLAN is called a VLAN interface. As a router, the ZyWALL routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

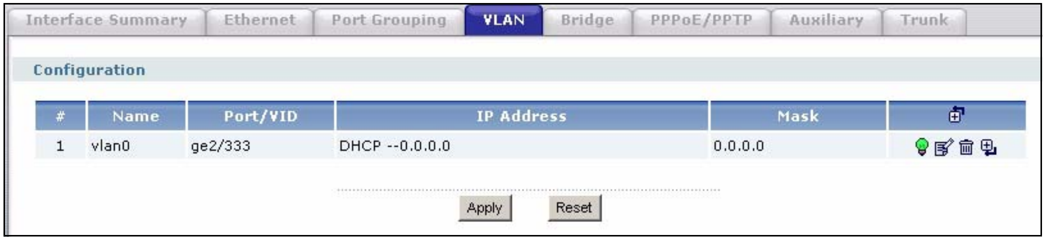
Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

10.4.3 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. To access this screen, click **Network** > **Interface** > **VLAN**.

Figure 132 Network > Interface > VLAN



#	Name	Port/VID	IP Address	Mask
1	vlan0	ge2/333	DHCP --0.0.0.0	0.0.0.0

Each field is explained in the following table.

Table 52 Network > Interface > VLAN

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.

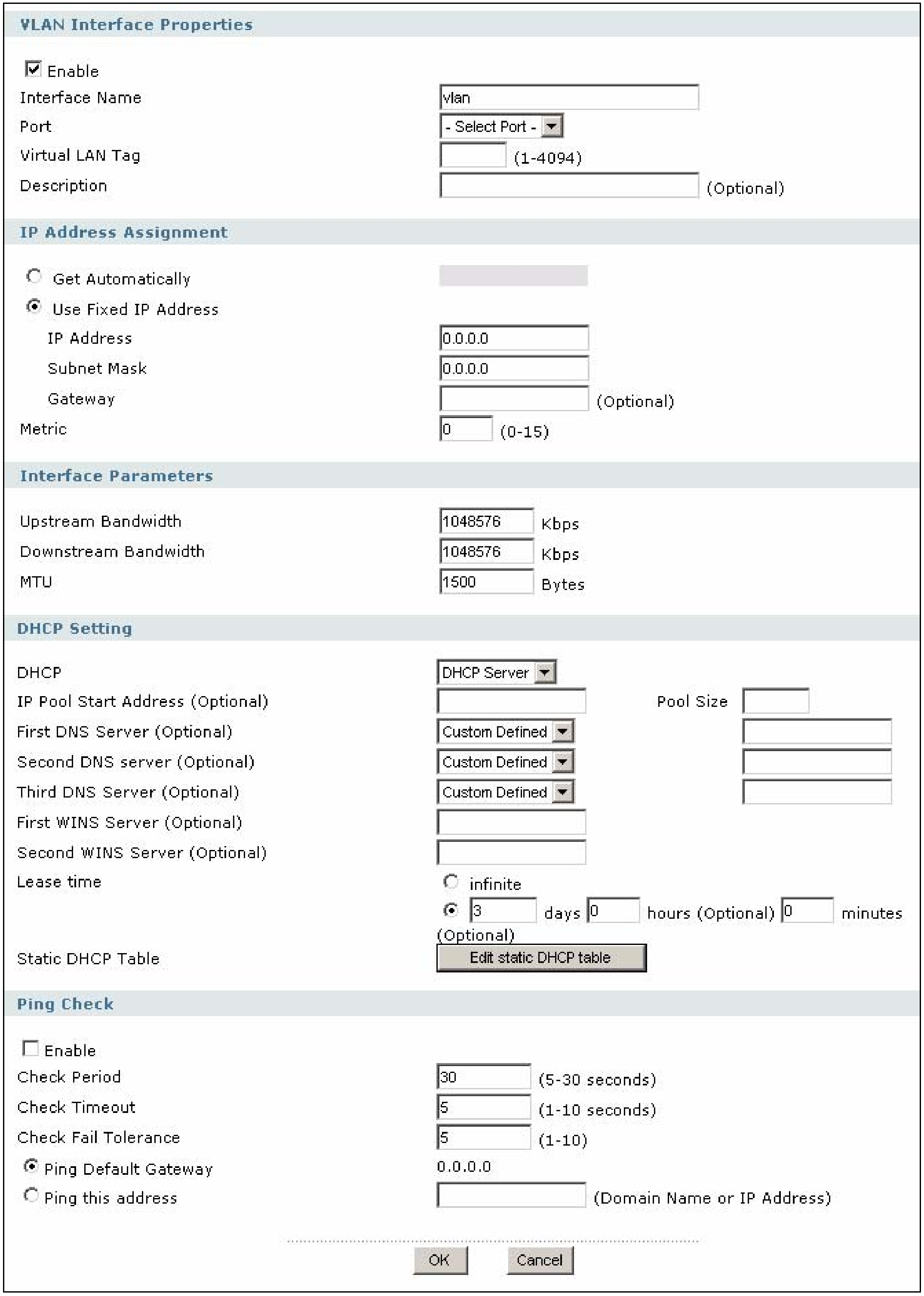
Table 52 Network > Interface > VLAN (continued)

LABEL	DESCRIPTION
Port/VID	For VLAN interfaces, this field displays • the Ethernet interface on which the VLAN interface is created • the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Add icon	This column lets you create, edit, remove, activate, and deactivate interfaces. To create a VLAN interface, click the **Add** icon at the top of the column. The **VLAN Add/Edit** screen appears. To create a virtual VLAN interface, click the **Add** icon next to the corresponding VLAN interface. The **Virtual Interface Add/Edit** screen appears. See Section 10.8 on page 217. To edit an interface, click the **Edit** icon next to it. The **VLAN Add/Edit** screen or **Virtual Interface Add/Edit** screen appears accordingly. To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4.4 VLAN Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and ping check for each VLAN interface. To access this screen, click the **Add** icon at the top of the **Add** column or click an **Edit** icon next to a VLAN interface in the **VLAN Summary** screen. The following screen appears.

Figure 133 Network > Interface > VLAN > Edit



VLAN Interface Properties

☑ Enable

Interface Name: vlan

Port: - Select Port -

Virtual LAN Tag: (1-4094)

Description: (Optional)

IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0-15)

Interface Parameters

Upstream Bandwidth: 1048576 Kbps

Downstream Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

DHCP Setting

DHCP: DHCP Server

IP Pool Start Address (Optional): Pool Size

First DNS Server (Optional): Custom Defined

Second DNS server (Optional): Custom Defined

Third DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):

Lease time: ○ infinite

● 3 days 0 hours (Optional) 0 minutes (Optional)

Static DHCP Table: Edit static DHCP table

Ping Check

☐ Enable

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

● Ping Default Gateway: 0.0.0.0

○ Ping this address: (Domain Name or IP Address)

Each field is explained in the following table.

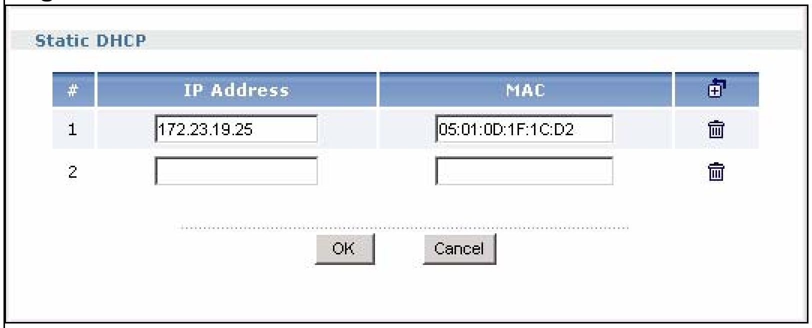
Table 53 Network > Interface > VLAN > Edit

LABEL	DESCRIPTION
VLAN Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the VLAN interface. The format is vlan*x*, where *x* is 0 - 31. For example, vlan0, vlan8, and so on.
Port	Select the Ethernet interface on which the VLAN interface runs.
Virtual LAN Tag	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group. See Chapter 33 on page 493.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Setting	

Table 53 Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
DHCP	Select what type of DHCP service the ZyWALL provides to the network. Choices are: **None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. You can specify these IP addresses two ways. **Custom Defined** - enter a static IP address **From ISP** - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.

Table 53 Network > Interface > VLAN > Edit (continued)

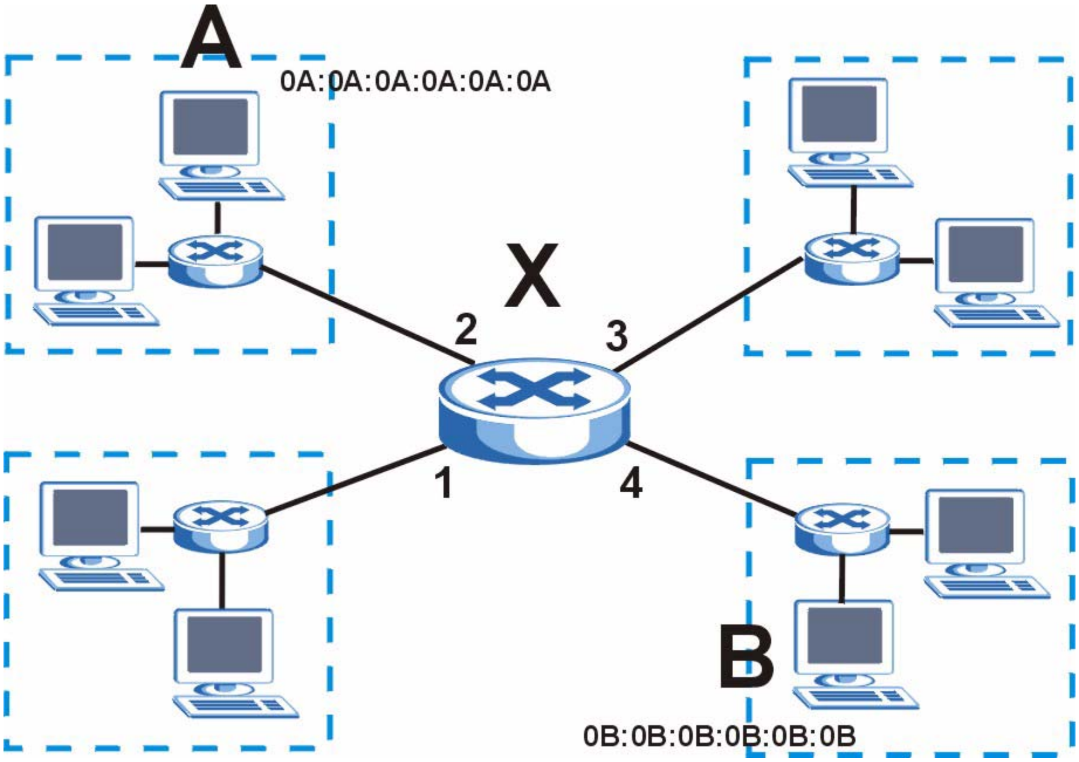
LABEL	DESCRIPTION
Edit static DHCP table	Click this if you want the ZyWALL to assign static IP addresses to computers. The **Static DHCP** screen appears. **Figure 134** Network > Interface > Edit > Edit static DHCP table  Static DHCP # | IP Address | MAC 1 | 172.23.19.25 | 05:01:0D:1F:1C:D2 2 | | OK Cancel The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns the IP address dynamically using the **IP Pool Start Address** and **Pool Size**. Note: You must click **OK** in the **Static DHCP** screen and then click **OK** in this screen to save your changes.
Ping Check	The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.
Enable	Select this to enable the ping check.
Check Period	Enter the number of seconds between ping attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Ping Default Gateway	Select this to ping the default gateway.
Ping this address	Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.

10.5 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

10.5.1 Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge X connects four network segments.



When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

Table 54 Example: Bridge Table After Computer A Sends a Packet to Computer B

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

Table 55 Example: Bridge Table After Computer B Responds to Computer A

MAC ADDRESS	PORT
`0A:0A:0A:0A:0A:0A`	2
`0B:0B:0B:0B:0B:0B`	4

10.5.2 Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the ZyWALL's interface for the resulting network.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the ZyWALL removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between ge1 and vlan1.

Table 56 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	ge1
210.211.1.0/24	ge1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	ge3
241.241.241.241/32	ge4
242.242.242.242/32	ge5

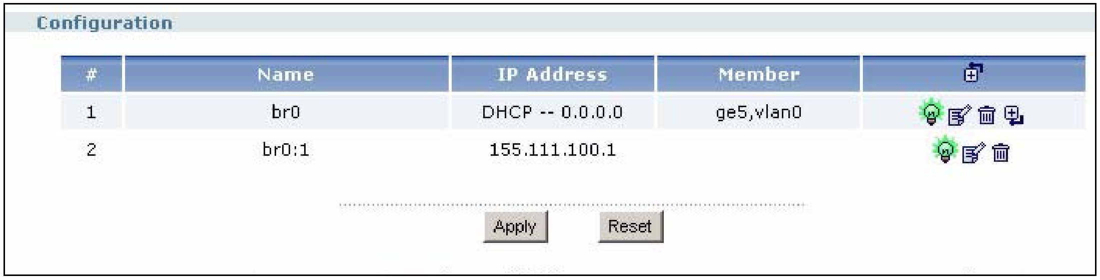
IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	ge3
241.241.241.241/32	ge4
242.242.242.242/32	ge5
250.250.250.0/23	br0

In this example, virtual Ethernet interface ge1:1 is also removed from the routing table when ge1 is added to br0. Virtual interfaces are automatically added to or remove from a bridge interface when the underlying interface is added or removed.

10.5.3 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. To access this screen, click **Network** > **Interface** > **Bridge**.

Figure 135 Network > Interface > Bridge



#	Name	IP Address	Member
1	br0	DHCP -- 0.0.0.0	ge5,vlan0
2	br0:1	155.111.100.1	

Each field is described in the following table.

Table 57 Network > Interface > Bridge

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.

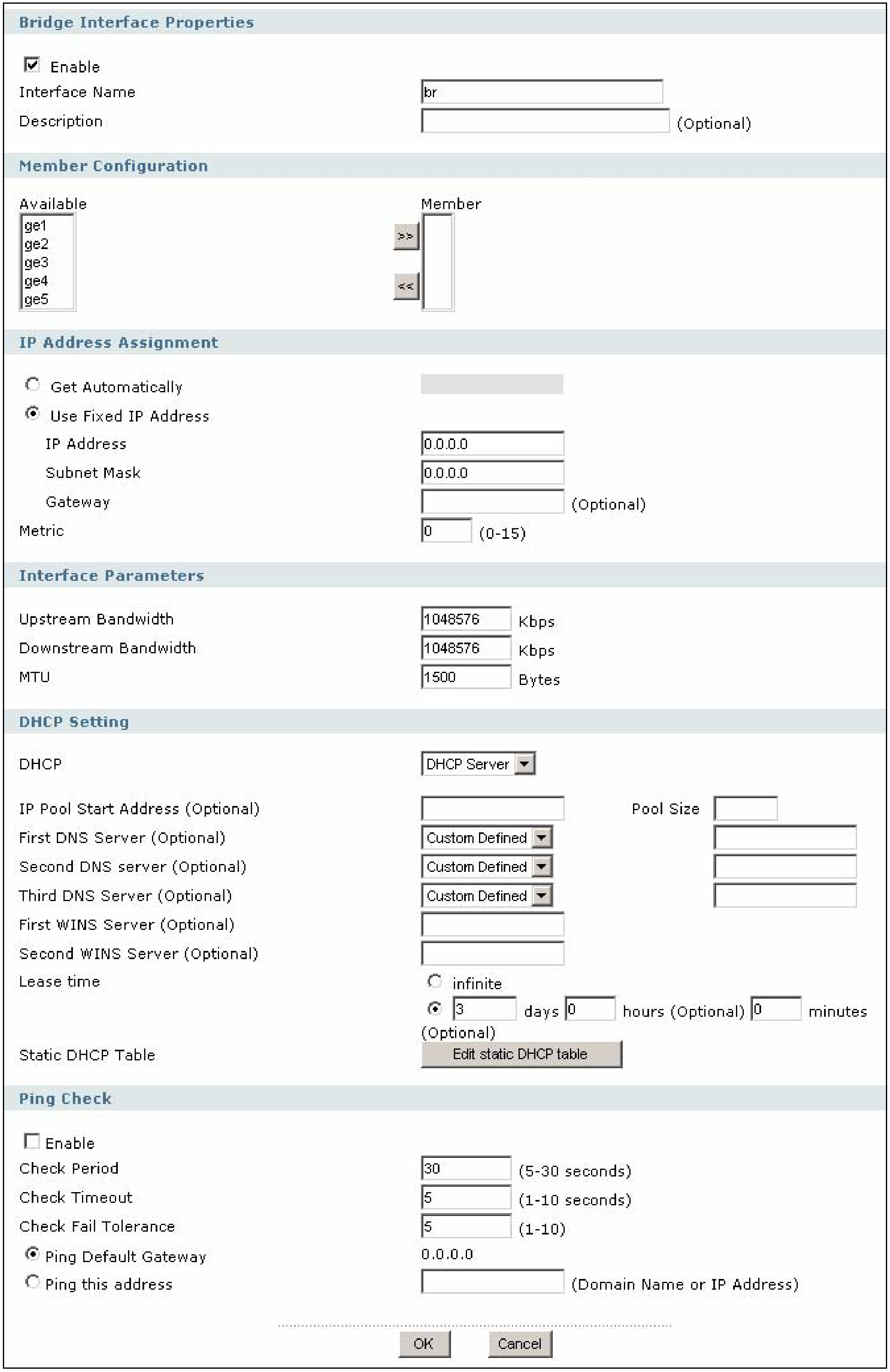
Table 57 Network > Interface > Bridge (continued)

LABEL	DESCRIPTION
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Add icon	This column lets you create, edit, remove, activate, and deactivate interfaces. To create a bridge interface, click the **Add** icon at the top of the column. The **Bridge Add/Edit** screen appears. To create a virtual interface, click the **Add** icon next to the corresponding bridge interface. The **Virtual Interface Add/Edit** screen appears. See Section 10.8 on page 217. To edit an interface, click the **Edit** icon next to it. The **Bridge Add/Edit** screen or **Virtual Interface Add/Edit** screen appears accordingly. To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

10.5.4 Bridge Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and ping check for each bridge interface. To access this screen, click the **Add** icon at the top of the **Add** column in the **Bridge Summary** screen, or click an **Edit** icon in the **Bridge Summary** screen. The following screen appears.

Figure 136 Network > Interface > Bridge > Edit



Bridge Interface Properties

☑ Enable

Interface Name: br

Description: (Optional)

Member Configuration

Available: ge1, ge2, ge3, ge4, ge5

Member:

IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0-15)

Interface Parameters

Upstream Bandwidth: 1048576 Kbps

Downstream Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

DHCP Setting

DHCP: DHCP Server

IP Pool Start Address (Optional): Pool Size

First DNS Server (Optional): Custom Defined

Second DNS server (Optional): Custom Defined

Third DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):

Lease time: ○ infinite

● 3 days 0 hours (Optional) 0 minutes (Optional)

Static DHCP Table: Edit static DHCP table

Ping Check

☐ Enable

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

● Ping Default Gateway 0.0.0.0

○ Ping this address (Domain Name or IP Address)

In this example, you are creating a new bridge. If you are editing a bridge, the **Interface Name** field is read-only. Each field is described in the table below.

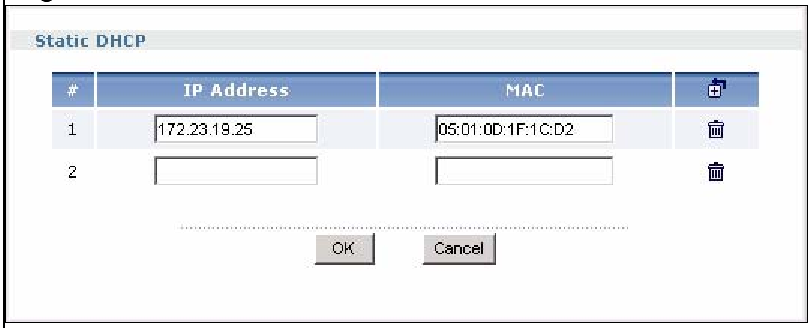
Table 58 Network > Interface > Bridge > Edit

LABEL	DESCRIPTION
Bridge Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%`– characters, and it can be up to 60 characters long.
Member Configuration	
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the **>>** arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the **<<** arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.

Table 58 Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Settings	
DHCP	Select what type of DHCP service the ZyWALL provides to the network. Choices are: **None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. You can specify these IP addresses two ways. **Custom Defined** - enter a static IP address **From ISP** - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.

Table 58 Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
Edit static DHCP table	Click this if you want the ZyWALL to assign static IP addresses to computers. The **Static DHCP** screen appears. **Figure 137** Network > Interface > Edit > Edit static DHCP table  Static DHCP # / IP Address / MAC 1 / 172.23.19.25 / 05:01:0D:1F:1C:D2 2 OK / Cancel The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns the IP address dynamically using the **IP Pool Start Address** and **Pool Size**. Note: You must click **OK** in the **Static DHCP** screen and then click **OK** in this screen to save your changes.
Ping Check	The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.
Enable	Select this to enable the ping check.
Check Period	Enter the number of seconds between ping attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Ping Default Gateway	Select this to ping the default gateway.
Ping this address	Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.

10.6 PPPoE/PPTP Interfaces

This section introduces PPPoE, PPTP, and PPPoE/PPTP interfaces and then explains the screens for PPPoE/PPTP interfaces.

10.6.1 PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections.

PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecure TCP/IP environments. It sets up two sessions.

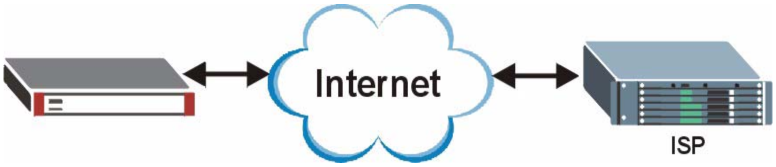
1. The first one runs on TCP port 1723. It is used to start and manage the second one.
2. The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

10.6.2 PPPoE/PPTP Interfaces Overview

In the ZyWALL, you may use PPPoE/PPTP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

Figure 138 Example: PPPoE/PPTP Interfaces



PPPoE/PPTP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP interfaces and other interfaces.

1. You must set up an ISP account before you create a PPPoE/PPTP interface.

   Each ISP account specifies the protocol (PPPoE or PPTP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP interface. You should not have to change any network policies.
2. You do not set up the subnet mask or gateway.

   PPPoE/PPTP interfaces are interfaces between the ZyWALL and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the ZyWALL always treats the ISP as a gateway.

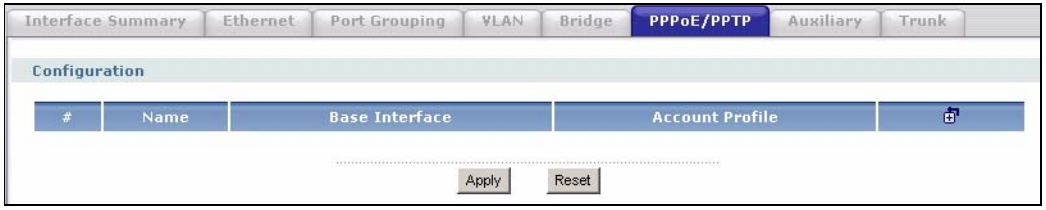
At the time of writing, it is possible to set up the IP address of the gateway (ISP) using CLI commands but not in the web configurator.

10.6.3 PPPoE/PPTP Interface Summary

You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lists every PPPoE/PPTP interface. To access this screen, click **Network** > **Interface** > **PPPoE/PPTP**.

Figure 139 Network > Interface > PPPoE/PPTP



Each field is described in the table below.

Table 59 Network > Interface > PPPoE/PPTP

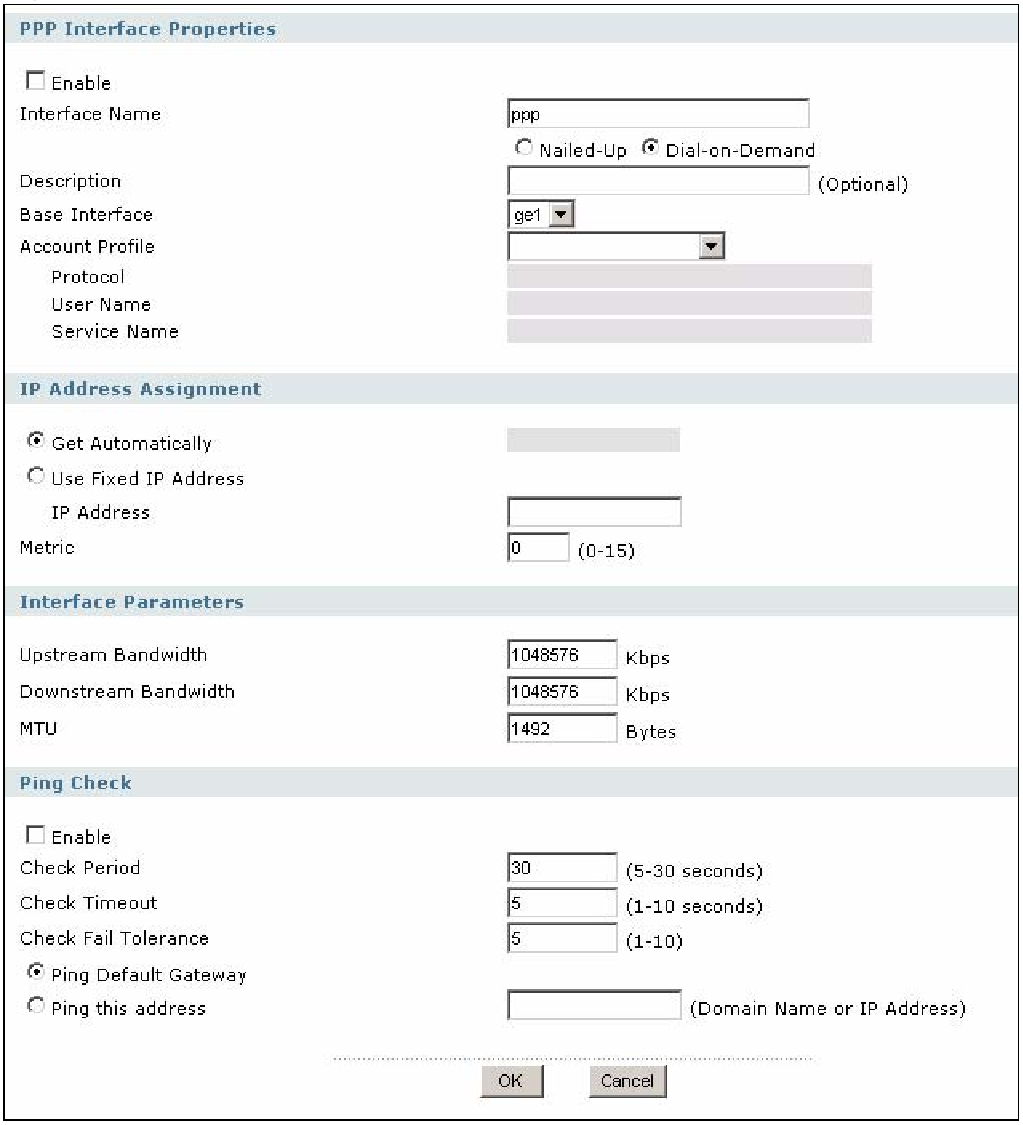
LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Add icon	This column lets you create, edit, remove, activate, deactivate, connect and disconnect interfaces. To create an interface, click the **Add** icon at the top of the column. The **PPPoE/PPTP Interface Add/Edit** screen appears. To edit an interface, click the **Edit** icon next to it. The **PPPoE/PPTP Interface Add/Edit** screen appears. To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change. To connect or disconnect an interface, click the **Connect** icon next to it. You might use this icon to test the interface or to manually establish the connection for a **Dial-on-Demand** PPPoE/PPTP interface.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

10.6.4 PPPoE/PPTP Interface Add/Edit

You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lets you configure new or existing PPPoE/PPTP interfaces. To access this screen, click the **Add** icon or an **Edit** icon in the **PPPoE/PPTP Interface Summary** screen.

Figure 140 Network > Interface > PPPoE/PPTP > Edit



PPP Interface Properties

☐ Enable	
Interface Name	ppp
	○ Nailed-Up ● Dial-on-Demand
Description	(Optional)
Base Interface	ge1 ▼
Account Profile	▼
Protocol	
User Name	
Service Name	

IP Address Assignment

● Get Automatically	
○ Use Fixed IP Address	
IP Address	
Metric	0 (0-15)

Interface Parameters

Upstream Bandwidth	1048576 Kbps
Downstream Bandwidth	1048576 Kbps
MTU	1492 Bytes

Ping Check

☐ Enable	
Check Period	30 (5-30 seconds)
Check Timeout	5 (1-10 seconds)
Check Fail Tolerance	5 (1-10)
● Ping Default Gateway	
○ Ping this address	(Domain Name or IP Address)

Each field is explained in the following table.

Table 60 Network > Interface > PPPoE/PPTP > Edit

LABEL	DESCRIPTION
PPP Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is ppp*x*, where *x* is 0 - 11. For example, ppp0, ppp7, and so on.
Nail_Up	Select this if the PPPoE/PPTP connection should always be up.
Dial-on-Demand	Select this if you want the ZyWALL to establish the PPPoE/PPTP connection only when there is traffic. You might select this if there is little traffic through the interface or if it costs money to keep the connection available.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Base Interface	Select the interface on which the PPPoE/PPTP interface runs. This interface can be an Ethernet interface, VLAN interface, or bridge interface. PPPoE/PPTP interfaces cannot run on Ethernet interfaces or VLAN interfaces that are used in bridge interfaces, however.
Account Profile	Select the ISP account that this PPPoE/PPTP interface uses. The drop-down box lists ISP accounts by name. Select **Create Object** to create a new ISP account (see Section 41.3 on page 564 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.

Table 60 Network > Interface > PPPoE/PPTP > Edit (continued)

LABEL	DESCRIPTION
Ping Check	The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.
Enable	Select this to enable the ping check.
Check Period	Enter the number of seconds between ping attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Ping Default Gateway	Select this to ping the default gateway.
Ping this address	Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.

10.7 Auxiliary Interface

This section introduces the auxiliary interface and then explains the screen for it.

10.7.1 Auxiliary Interface Overview

Use the auxiliary interface to dial out from the ZyWALL’s auxiliary port. For example, you might use this interface as a backup WAN interface.

You have to connect an external modem to the ZyWALL’s auxiliary port to use the auxiliary interface.

You have to connect an external modem to the auxiliary port.

The ZyWALL uses the auxiliary interface to dial out in two situations.

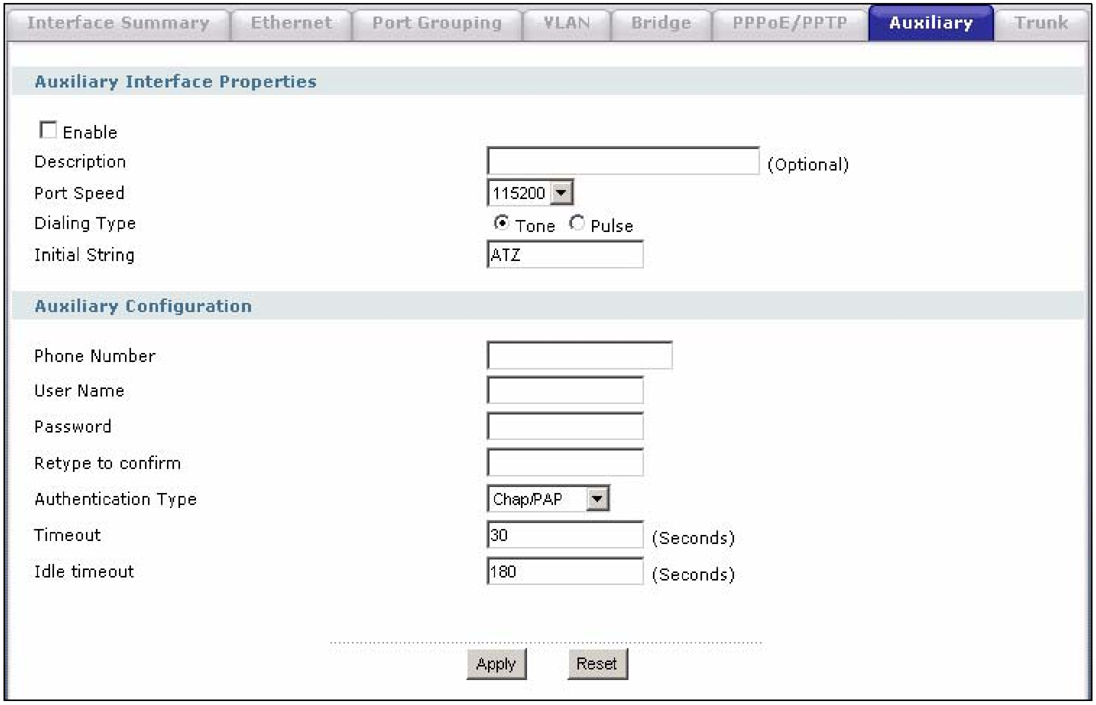
1. You click the **Connect** icon on the ZyWALL **Status** screen.
2. The load auxiliary interface must connect to satisfy load-balancing requirements. You have to add the auxiliary interface to a trunk first.

When the ZyWALL hangs up the call, it drops the Data Terminal Ready (DTR) signal and issues the command `ATH`.

10.7.2 Auxiliary

Use the **Auxiliary** screen to configure the ZyWALL’s auxiliary interface. Click **Network** > **Interface** > **Auxiliary** to open it.

Figure 141 Network > Interface > Auxiliary



Auxiliary Interface Properties

☐ Enable

Description (Optional)

Port Speed 115200

Dialing Type ● Tone ○ Pulse

Initial String ATZ

Auxiliary Configuration

Phone Number

User Name

Password

Retype to confirm

Authentication Type Chap/PAP

Timeout 30 (Seconds)

Idle timeout 180 (Seconds)

Each field is described in the table below.

Table 61 Network > Interface > Auxiliary

LABEL	DESCRIPTION
Auxiliary Interface Properties	
Enable	Select this to turn on the auxiliary dial up interface. The interface does not dial out, however, unless it is part of a trunk and load-balancing conditions are satisfied.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Port Speed	Select the speed of the connection between the ZyWALL and external computer.
Dialing Type	**Tone** - select this if the telephone uses tone-based dialing. **Pulse** - select this if the telephone uses pulse-based dialing.
Initial String	Enter the AT command string to initialize the external modem. `ATZ` is the most common string, but you should check the manual for the external modem for additional commands.
Auxiliary Configuration	
Phone Number	Enter the phone number to dial here. You can use 1-20 numbers, commas (,), or plus signs (+). Use a comma to pause during dialing. Use a plus sign to tell the external modem to make an international call.
User Name	Enter the user name required for authentication.
Password	Enter the password required for authentication.
Retype to confirm	Enter the password again to make sure you have not typed it incorrectly.

Table 61 Network > Interface > Auxiliary (continued)

LABEL	DESCRIPTION
Authentication Type	Select the authentication protocol to use for outgoing calls. Choices are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP, as requested by the computer you are dialing. **CHAP** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accepts PAP only. **MSCHAP** - Your ZyWALL accepts MSCHAP only. **MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only.
Timeout	Type the number of seconds the ZyWALL tries to set up a connection before it stops. Allowed values are 30 - 120.
Idle timeout	Type the number of seconds the ZyWALL should wait for traffic before it automatically disconnects the connection. Set this field to zero to disable the idle timeout. Allowed values are 0 - 360.

10.8 Virtual Interfaces

Use virtual interfaces to tell the ZyWALL where to route packets. Virtual interfaces can also be used in VPN gateways (see Chapter 20 on page 291) and VRRP groups (see Chapter 33 on page 493).

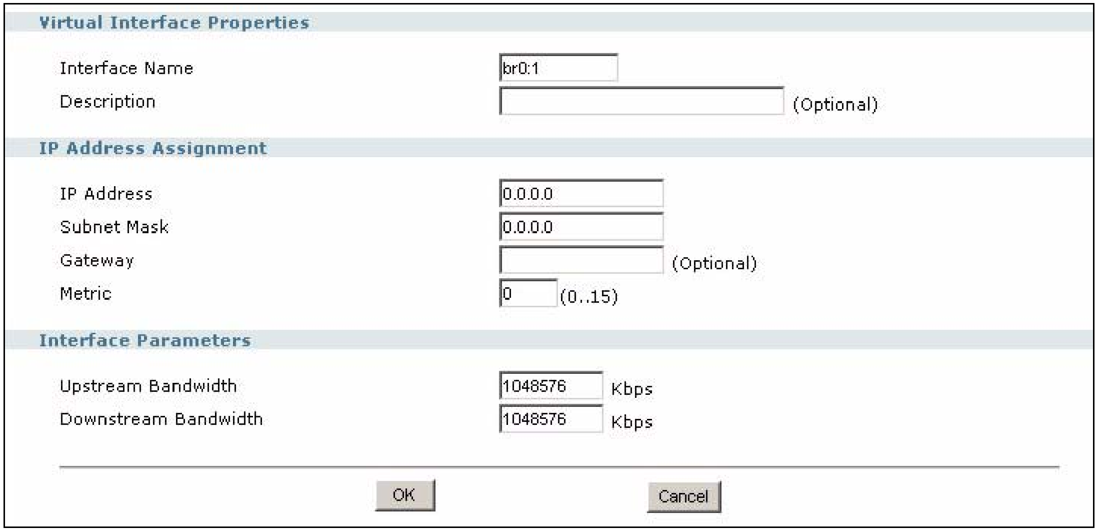
Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, firewall rules) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. Like other interfaces, you can restrict bandwidth through virtual interfaces, but you cannot change the MTU. The virtual interface uses the same MTU that the underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

10.8.1 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click an **Add** icon next to an Ethernet interface, VLAN interface, or bridge interface in the respective interface summary screen.

Figure 142 Network > Interface > Add



Virtual Interface Properties

Interface Name: br0:1

Description: (Optional)

IP Address Assignment

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0..15)

Interface Parameters

Upstream Bandwidth: 1048576 Kbps

Downstream Bandwidth: 1048576 Kbps

Each field is described in the table below.

Table 62 Network > Interface > Add

LABEL	DESCRIPTION
Virtual Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Properties	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.

11

Trunks

This chapter shows you how to configure trunks on your ZyWALL. See Section 5.4.3 on page 115 for related information on these screens.

11.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface’s connection goes down, the ZyWALL sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The ZyWALL can balance the load between multiple connections (see Section 11.3 on page 219). If one interface's connection goes down, the ZyWALL can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface’s connection goes down, the ZyWALL can still send its traffic through another interface.

11.2 Trunk Scenario Examples

Suppose one of the ZyWALL's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface’s connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

11.3 Load Balancing Introduction

On the ZyWALL, load balancing is the process of dividing traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization.

Maybe you have two connections with different bandwidths. For jitter-sensitive traffic (like video for example), you could set up a trunk group that uses spillover or weighted round robin load balancing to make sure that most of the jitter-sensitive traffic goes through the higher-bandwidth interface.

For some traffic connections, you might want to use least load first load balancing in order to even out the distribution of the traffic load.

11.4 Load Balancing Algorithms

The following sections describe the load balancing algorithms that the ZyWALL can use to decide which interface the traffic (from the LAN) should use for a session[3]. The available bandwidth you configure on the ZyWALL refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

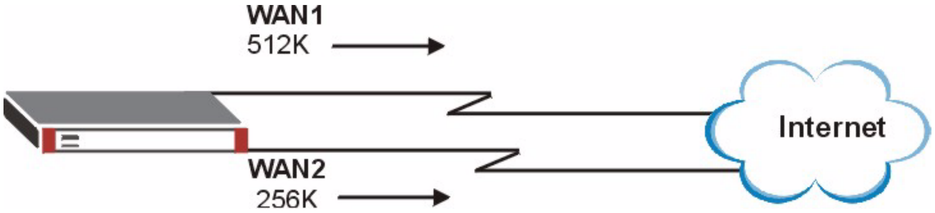
11.4.1 Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

11.4.1.1 Least Load First Example 1

The following example shows two WAN interfaces on the ZyWALL connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

Figure 143 Least Load First Example 1



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The ZyWALL calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the ZyWALL will send the subsequent new session traffic through WAN 2.

Table 63 Least Load First: Example 1

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

---

[3] In the load balancing section, a session may refer to normal connection-oriented, UDP and SNMP2 traffic.

11.4.2 Weighted Round Robin

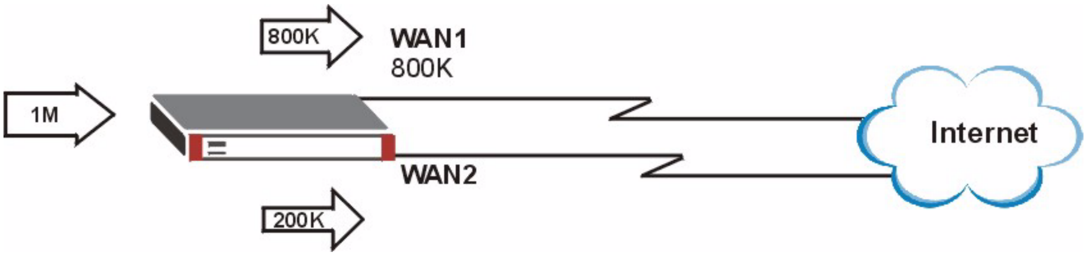
Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the ZyWALL to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more of the traffic than an interface with a smaller weight.

This algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the ZyWALL to distribute the network traffic between the two interfaces by setting the weight of WAN1 and WAN2 to 2 and 1 respectively. The ZyWALL assigns the traffic of two sessions to WAN1 for every session's traffic assigned to WAN2.

Figure 144 Weighted Round Robin Algorithm Example



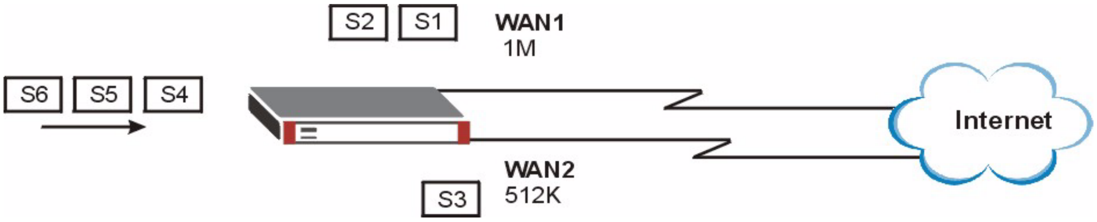
11.4.3 Spillover

With the spillover load balancing algorithm, the ZyWALL sends network traffic to the first interface in the trunk member list until the interface’s maximum allowable load is reached, then the ZyWALL sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

In cases where the first interface in the trunk member list uses an unlimited access Internet connection and the secondary WAN uses a per-use timed access plan, the ZyWALL will only use the next interface in the trunk member list when the traffic load exceeds the threshold on the first interface. This allows you to fully utilize the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

In the following example figure, the upper threshold of the first interface is set to 800K. The ZyWALL sends network traffic of new sessions that exceed this limit to the secondary WAN interface.

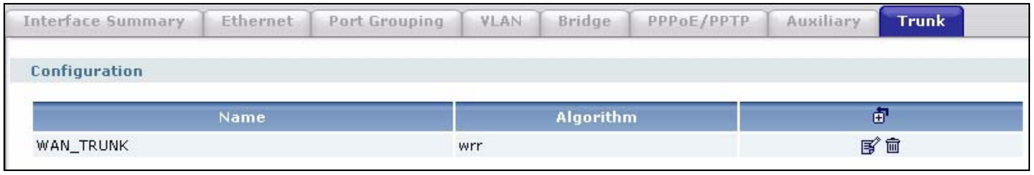
Figure 145 Spillover Algorithm Example


S2
S1
WAN1
1M
S6
S5
S4
Internet
WAN2
512K
S3

11.5 Trunk Summary

Click **Network** > **Interface** > **Trunk** to open the **Trunk** screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 146 Network > Interface > Trunk


Interface Summary
Ethernet
Port Grouping
VLAN
Bridge
PPPoE/PPTP
Auxiliary
Trunk
Configuration

Name	Algorithm	
WAN_TRUNK	wrr	

The following table describes the items in this screen.

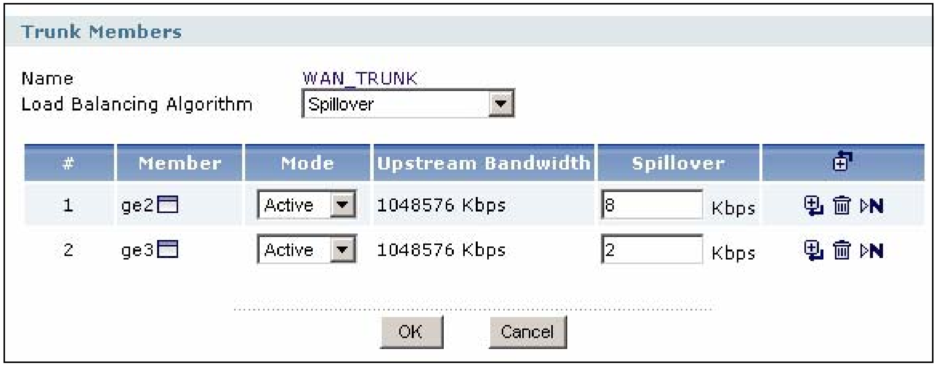
Table 64 Network > Interface > Trunk

LABEL	DESCRIPTION
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method that the trunk is set to use.
Add icon	This column lets you create, edit and remove trunks. To create a trunk, click the **Add** icon at the top of the column. The **Trunk Members** screen appears. To edit a trunk, click the **Edit** icon next to it. The **Trunk Members** screen appears. To remove a trunk, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.

11.6 Configuring a Trunk

Click **Network** > **Interface** > **Trunk** and then the **Add** (or **Edit**) icon to open the **Trunk Edit** screen.

Figure 147 Network > Interface > Trunk > Edit



Name: WAN_TRUNK
Load Balancing Algorithm: Spillover

#	Member	Mode	Upstream Bandwidth	Spillover
1	ge2	Active	1048576 Kbps	8 Kbps
2	ge3	Active	1048576 Kbps	2 Kbps

Each field is described in the table below.

Table 65 Network > Interface > Trunk > Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. Weighted round robin is activated only when the first group member interface has more traffic than it can handle. Select **Least Load First** to send new session traffic through the least utilized trunk member. Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this icon to open a screen where you can select an interface to be a group member. If you select an interface that is part of another Ethernet interface, the ZyWALL does not send traffic through the interface as part of the trunk. For example, if you have physical port 5 in the ge2 representative interface, you must select interface ge2 in order to send traffic through port 5 as part of the trunk. If you select interface ge5 as a member here, the ZyWALL will not send traffic through port 5 as part of the trunk.
Mode	Select **Active** to have the ZyWALL always attempt to use this connection. Select **Passive** to have the ZyWALL only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the ZyWALL sends through each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more traffic the ZyWALL sends through that interface.
Downstream Bandwidth	This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to allow to come in through the interface per second.
Upstream Bandwidth	This field displays with the least load first or spillover load balancing algorithm.It displays the maximum number of kilobits of data the ZyWALL is to send out through the interface per second.

Table 65 Network > Interface > Trunk > Edit (continued)

LABEL	DESCRIPTION
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the ZyWALL sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The ZyWALL uses the group member interfaces in the order that they are listed.
Add icon	This column lets you add, remove and move trunk members. To add an interface to the trunk, click an **Add** icon. The **Trunk Member Select** screen appears. To remove an interface from a trunk, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so. To move an interface to a different number in the list, click the **Move** icon next to it. In the field that appears, specify the number to which you want to move the interface.

12

Policy and Static Routes

This chapter shows you how to configure policies for IP routing and static routes on your ZyWALL. See Section 5.4.10 on page 117 for related information on the policy route screens.

12.1 Policy Route

Traditionally, routing is based on the destination address only and the ZyWALL takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

12.1.1 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – Organizations can allocate bandwidth to traffic that matches the routing policy and prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ZyWALL performs NAT by default for traffic going to or from the **ge1** interface. Routing policy’s SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

12.2 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

12.2.1 NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

12.2.2 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set the port(s) and IP address to forward a service (coming in from the remote server) to a client computer. The problem is that port forwarding only forwards a service to a single IP address. In order to use the same service on a different computer, you have to manually replace the client computer's IP address with another client computer's IP address.

Port triggering allows the client computer to take turns using a service dynamically. Whenever a client computer’s packets match the routing policy, it can use the pre-defined port triggering setting to connect to the remote server without manually configuring a port forwarding rule for each client computer.

Port triggering is used especially when the remote server responses using a different port from the port the client computer used to request a service. The ZyWALL records the IP address of a client computer that sends traffic to a remote server to request a service (incoming service). When the ZyWALL receives a new connection (trigger service) from the remote server, the ZyWALL forwards the traffic to the IP address of the client computer that sent the request.

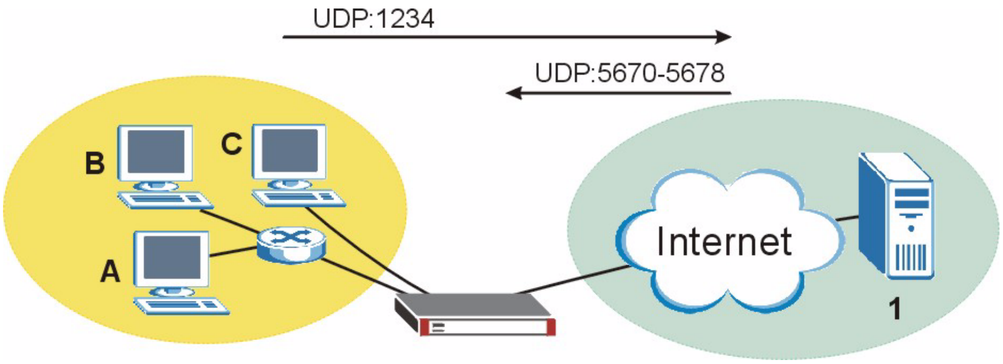
You need to create a firewall rule to allow an incoming service before using a port triggering rule.

In the following example, you configure two services for port triggering:

Incoming service: Game (UDP: 1234)
Trigger service: Game-1 (UDP: 5670-5678)

1. Computer **A** wants to play a multiplayer online game and tries to connect to game server **1** using port 1234. The ZyWALL records the IP address of computer **A** when the packets match a policy with SNAT configured.
2. Game server **1** responds using a port number ranging between 5670 - 5678. The ZyWALL allows and forwards the traffic to computer **A**.
3. Computer **A** and game server **1** are connected to each other until the connection is closed or times out. Any other computers (such as **B** or **C**) cannot connect to remote server **1** using the same port triggering rule as computer **A** unless they are using a different next hop (gateway, outgoing interface, VPN tunnel or trunk) from computer **A** or until the connection is closed or times out.

Figure 148 Trigger Port Forwarding Example



12.2.3 Maximize Bandwidth Usage

The maximize bandwidth usage option allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each policy route gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the policy routes) depending on how many policy routes require more bandwidth and on their priority levels. When only one policy route requires more bandwidth, the ZyWALL gives the extra bandwidth to that policy route.

When multiple policy routes require more bandwidth, the ZyWALL gives the highest priority policy routes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority policy routes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among policy routes with the same priority level.

12.2.4 Reserving Bandwidth for Non-Bandwidth Class Traffic

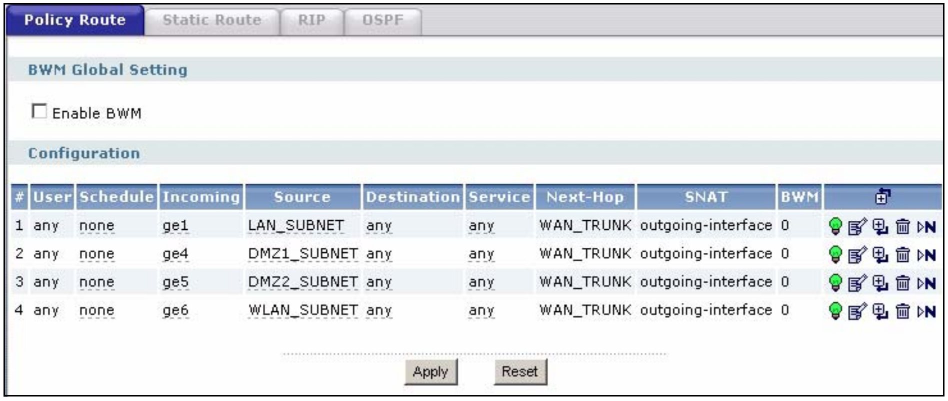
Do the following three steps to configure the ZyWALL to allow bandwidth for traffic that does not match a policy route.

1 Leave some of the interface's bandwidth unbudgeted.
2 Do not enable the **Maximize Bandwidth Usage** option in the policy routes.

12.3 IP Routing Policy Setup

Click **Network > Routing** to open the **Policy Route** screen.

Figure 149 Network > Routing > Policy Route



BWM Global Setting

☐ Enable BWM

Configuration

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM
1	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0
2	any	none	ge4	DMZ1_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0
3	any	none	ge5	DMZ2_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0
4	any	none	ge6	WLAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0

The following table describes the labels in this screen.

Table 66 Network > Routing > Policy Route

LABEL	DESCRIPTION
Enable BWM	This is a global setting for enabling or disabling bandwidth management on the ZyWALL. You must enable this setting to have individual policy routes or application patrol policies apply bandwidth management. This same setting also appears in the **AppPatrol > General** screen. Enabling or disabling it in one screen also enables or disables it in the other screen.
#	This is the number of an individual policy route.
User	This is the name of the user (group) object from which the packets are sent. **any** means all users.
Schedule	This is the name of the schedule object. **none** means the route is active at all times if enabled.
Incoming	This is the interface on which the packets are received.
Source	This is the name of the source IP address (group) object. **any** means all IP addresses.
Destination	This is the name of the destination IP address (group) object. **any** means all IP addresses.
Service	This is the name of the service object. **any** means all services.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
SNAT	This is the source IP address that the route uses. It displays **none** if the ZyWALL does not perform NAT for this route.
BWM	This is the maximum bandwidth allotted to the policy. **0** means there is no bandwidth limitation for this route.

Table 66 Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
Add icon	Click the **Add** icon in the heading row to add a new first entry. The **Active** icon displays whether the rule is enabled or not. Click the **Active** icon to activate or deactivate the policy. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the routing policy on the ZyWALL. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Remove** icon to delete an existing routing policy from the ZyWALL. A window displays asking you to confirm that you want to delete the routing policy. In a numbered list, click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

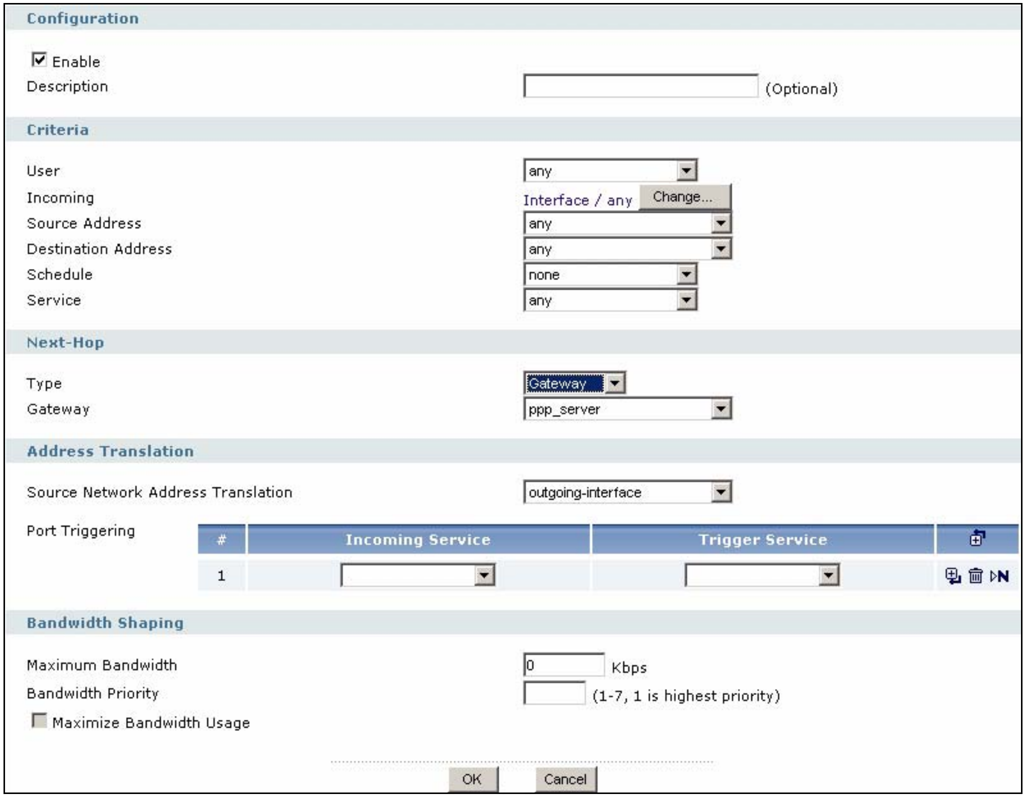
12.4 Policy Route Edit

Click **Network** > **Routing** to open the **Policy Route** screen. Then click the **Add** or **Edit** icon to open the **Policy Route Edit** screen.

Configure NAT loopback if you have a virtual server that local users will use a domain name to access.

See Section 6.7 on page 151 for an example of NAT loopback.

Figure 150 Network > Routing > Policy Route > Edit



☑ Enable

Description (Optional)

User any

Incoming Interface / any Change...

Source Address any

Destination Address any

Schedule none

Service any

Type Gateway

Gateway ppp_server

Source Network Address Translation outgoing-interface

Port Triggering

#	Incoming Service	Trigger Service
1		

Maximum Bandwidth 0 Kbps

Bandwidth Priority (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

The following table describes the labels in this screen.

Table 67 Network > Routing > Policy Route > Edit

LABEL	DESCRIPTION
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent. Select **Create Object** to configure a new user account (see Section 34.2.1 on page 506 for details).
Incoming Interface	Click **Change...** to select an interface or VPN tunnel through which the incoming packets are received.
Source Address	Select a source IP address object or select **Create Object** to configure a new one.
Destination Address	Select a destination IP address object or select **Create Object** to configure a new one.
Schedule	Select a schedule or select **Create Object** to configure a new one (see Chapter 37 on page 527 for details). **none** means the route is active at all times if enabled.
Service	Select a service or service group from the drop-down list box. Select **Create Object** to add a new service. See Section 36.2.1 on page 523 for more information.
Next-Hop	

Table 67 Network > Routing > Policy Route > Edit (continued)

LABEL	DESCRIPTION
Type	Select **Auto** to have the ZyWALL use the routing table to find a next-hop and forward the matched packets automatically. Select **Gateway** to route the matched packets to the next-hop router or switch you specified in the **Gateway** field. You have to set up the next-hop router or switch as a HOST address object first. Select **VPN Tunnel** to route the matched packets via the specified VPN tunnel. Select **Trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select **Interface** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select **Gateway** in the **Type** field. Select a HOST address object. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your ZyWALL's interface(s).
VPN Tunnel	This field displays when you select **VPN Tunnel** in the **Type** field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the ZyWALL directly.
Trunk	This field displays when you select **Trunk** in the **Type** field. Select a trunk group to have the ZyWALL send the packets via the interfaces in the group.
Interface	This field displays when you select **Interface** in the **Type** field. Select an interface to have the ZyWALL send traffic that matches the policy route through the specified interface.
Address Translation	
Source Network Address Translation	Select **none** to not use NAT for the route. Select **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. If you select **outgoing-interface**, you can also configure port trigger settings for this interface. Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route. Select **Create Object** to configure a new address (group) to use as the source IP address(es) of the packets that match this route.
Port Triggering	
#	This is the rule index number.
Incoming Service	Select the service that the client computer sends to a remote server. The incoming service should have the same service or protocol type as what you configured in the **Service** field.
Trigger Service	Select a service that a remote server sends. It causes (triggers) the ZyWALL to forward the traffic (received on the **outgoing interface**) to the client computer that requested the service.
Add icon	Click the **Add** icon in the heading row to add a new first entry. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. In a numbered list, click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.

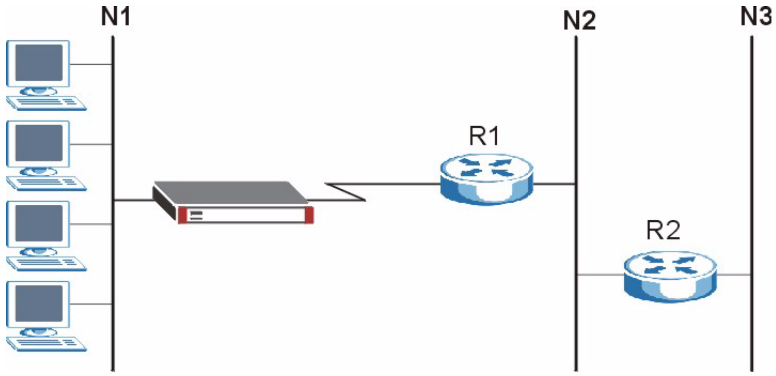
Table 67 Network > Routing > Policy Route > Edit (continued)

LABEL	DESCRIPTION
Bandwidth Shaping	This allows you to allocate bandwidth to a route and prioritize traffic that matches the routing policy. You must also enable bandwidth management in the main policy route screen (**Network > Routing > Policy Route**) in order to apply bandwidth shaping.
Maximum Bandwidth	Specify the maximum bandwidth (from 1 to 1048576) allowed for the route in kbps. If you enter **0** here, there is no bandwidth limitation for the route. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Bandwidth Priority	Enter a number between 1 and 7 to set the priority for traffic. The smaller the number, the higher the priority. If you set the maximum bandwidth to **0**, the bandwidth priority will be changed to **0** after you click **OK**. That means the route has the highest priority and will get all the bandwidth it needs up to the maximum available. A route with higher priority is given bandwidth before a route with lower priority. If you set routes to have the same priority, then bandwidth is divided equally amongst those routes.
Maximize Bandwidth Usage	Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the policy routes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see Section 12.2.4 on page 227).
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

12.5 IP Static Routes

The ZyWALL has no knowledge of the networks beyond the network that is directly connected to the ZyWALL. For instance, the ZyWALL knows about network **N2** in the following figure through gateway **R1**. However, the ZyWALL is unable to route a packet to network **N3** because it doesn't know that there is a route through the same gateway **R1** (via gateway **R2**). Static routes are for you to tell the ZyWALL about the networks beyond the network connected to the ZyWALL directly.

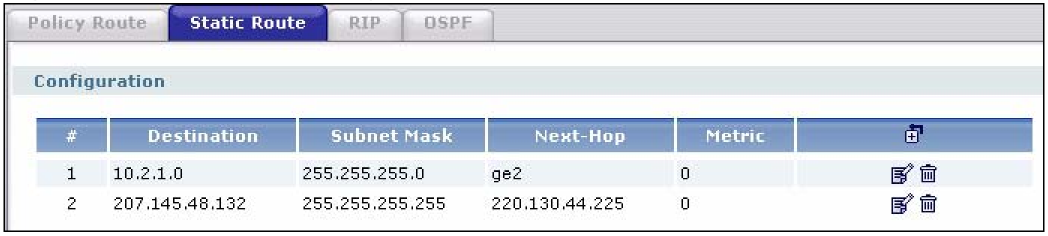
Figure 151 Example of Static Routing Topology



12.6 Static Route Summary

Click **Network** > **Routing** > **Static Route** to open the **Static Route** screen.

Figure 152 Network > Routing > Static Route



#	Destination	Subnet Mask	Next-Hop	Metric
1	10.2.1.0	255.255.255.0	ge2	0
2	207.145.48.132	255.255.255.255	220.130.44.225	0

The following table describes the labels in this screen.

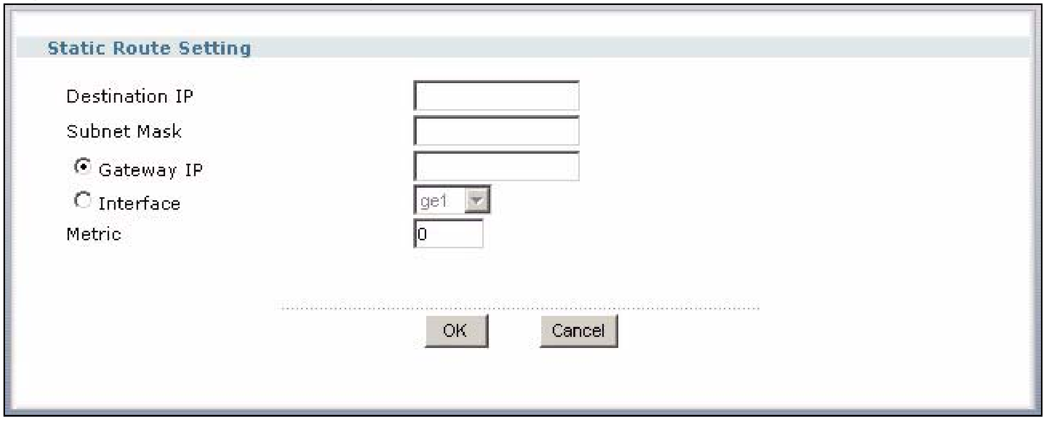
Table 68 Network > Routing > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has.
Add icon	Click the **Add** icon to go to the screen where you can set up a static route on the ZyWALL. Click the **Edit** icon to go to the screen where you can edit the static route on the ZyWALL. Click the **Remove** icon to delete an existing static route from the ZyWALL. A window displays asking you to confirm that you want to delete the routing policy.

12.7 Edit a Static Route

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 153 Network > Routing > Static Route > Edit



Destination IP
Subnet Mask
● Gateway IP
○ Interface: ge1
Metric: 0

The following table describes the labels in this screen.

Table 69 Network > Routing > Static Route > Edit

LABEL	DESCRIPTION
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	Enter the IP subnet mask here.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

13

Routing Protocols

This chapter describes how to set up RIP and OSPF routing protocol settings for the ZyWALL. First, it provides an overview of RIP and OSPF, and, then, it introduces the RIP and OSPF screens used to configure routing protocols. See Section 5.5 on page 122 for related information on these screens.

13.1 Routing Protocols Overview

Routing protocols give the ZyWALL routing information about the network from other routers. The ZyWALL then stores this routing information in the routing table, which it uses when it makes routing decisions. In turn, the ZyWALL can also provide routing information via routing protocols to other routers.

The ZyWALL supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 70 on page 235, and they are discussed further in the next two sections.

Table 70 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metric	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

13.1.1 RIP Overview

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

In the ZyWALL, you can configure two sets of RIP settings before you can use it in an interface.

First, the **Authentication** field specifies how to verify that the routing information that is received is the same routing information that is sent. This is discussed in more detail in Section 13.1.2 on page 236.

Second, the ZyWALL can also **redistribute** routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the **Metric** field to specify the cost in RIP terms.

RIP uses UDP port 520.

13.1.2 Authentication Types

Authentication is used to guarantee the integrity, but not the confidentiality, of routing updates. The transmitting router uses its key to encrypt the original message into a smaller message, and the smaller message is transmitted with the original message. The receiving router uses its key to encrypt the received message and then verifies that it matches the smaller message sent with it. If the received message is verified, then the receiving router accepts the updated routing information. The transmitting and receiving routers must have the same key.

The ZyWALL supports three authentication methods for RIP and OSPF routing protocols:

- **None** - no authentication is used.
- **Text** – authentication using a plain text password, and the (unencrypted) password is sent over the network. This method is usually used temporarily to prevent network problems.
- **MD5** – authentication using an MD5 password and authentication ID.

MD5 is an authentication method that produces a 128-bit checksum, called a message-digest, for each packet. It also includes an authentication ID, which can be set to any value between 1 and 255. The ZyWALL only accepts packets if these conditions are satisfied.

- The packet's authentication ID is the same as the authentication ID of the interface that received it.
- The packet's message-digest is the same as the one the ZyWALL calculates using the MD5 password.

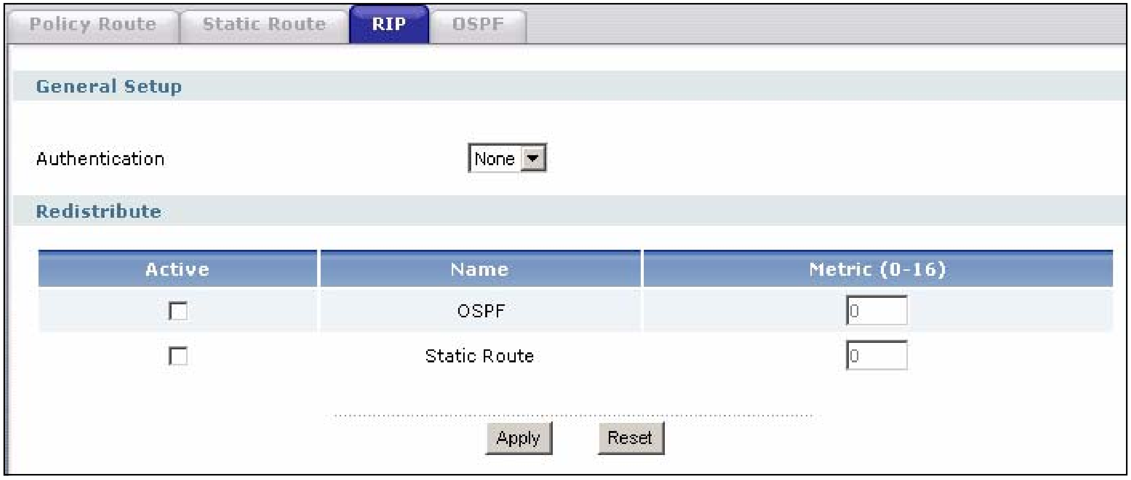
For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces. For OSPF, the ZyWALL supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated **Authentication Type** field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information.

13.2 RIP Screen

The **RIP** screen is used to specify the authentication method, and it is used to maintain the policies for redistribution.

To access this screen, login to the web configurator. When the main screen appears, click **Network** > **Routing > RIP** to open the following screen.

Figure 154 Network > Routing > RIP



The following table describes the labels in this screen.

Table 71 Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	
Authentication	Select the authentication method used in the RIP network. Choices are: **None**, **Text**, and **MD5**.
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Redistribute	
Active	Select this check box to advertise routes that were learned from the indicated **Name**.
Name	This field displays other sources of routing information that the ZyWALL can advertise in the RIP network.
Metric	Type the cost for routes provided by the indicated source. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.

13.3 OSPF Overview

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.

- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

13.3.1 OSPF Areas

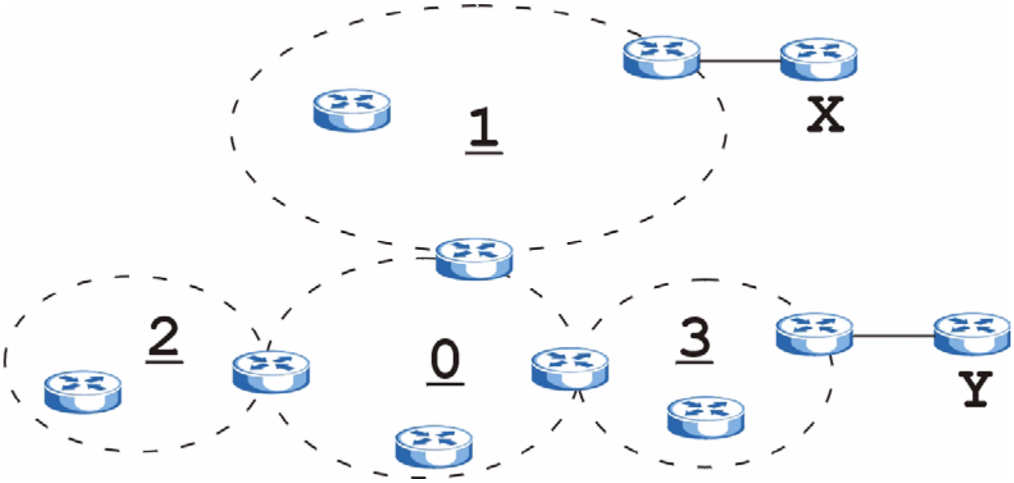
An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 155 OSPF: Types of Areas



This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

13.3.2 OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.
- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

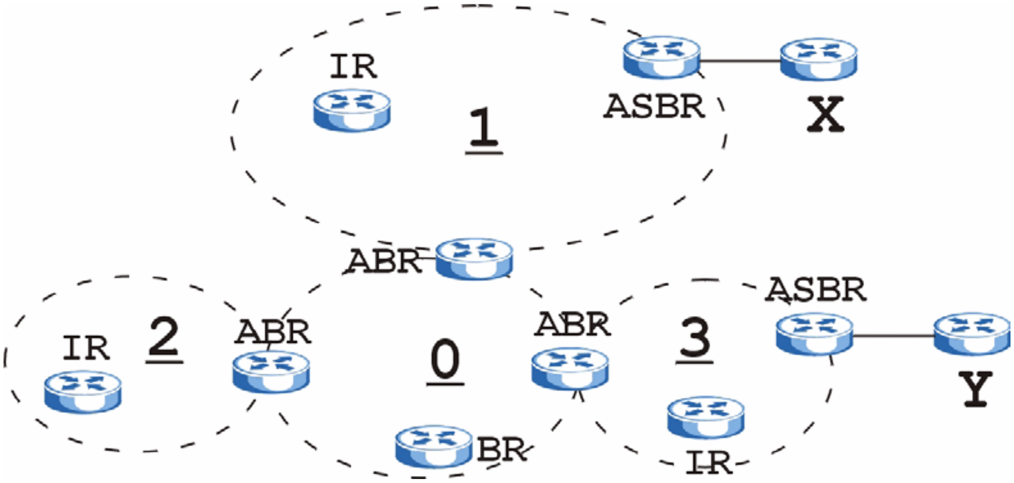
Table 72 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	Yes

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 156 OSPF: Types of Routers



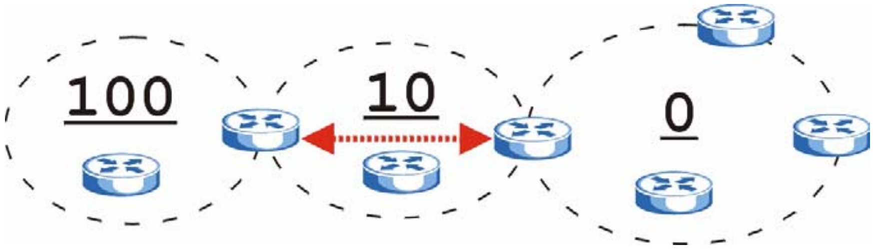
In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

13.3.3 Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 157 OSPF: Virtual Link



In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

13.3.4 OSPF Configuration

Follow these steps when you configure OSPF on the ZyWALL.

1 Enable OSPF.

2 Set up the OSPF areas.

3 Configure the appropriate interfaces. See Section 10.2.1 on page 184.

4 Set up virtual links, as needed.

13.4 OSPF Screens

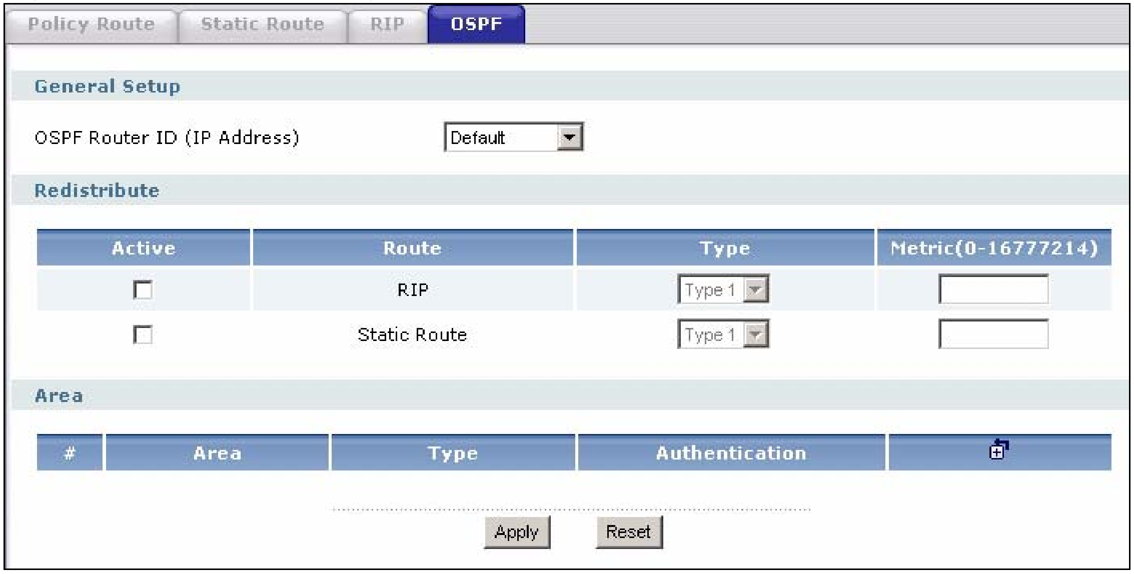
The OSPF screens are used to specify the ID the ZyWALL uses in the OSPF AS and to maintain the policies for redistribution. In addition, they are also used to create, maintain, and remove OSPF areas.

13.4.1 OSPF Summary

The **OSPF** screen is used to specify the OSPF router and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the **OSPF Add/Edit** screen to add or edit them.

To access this screen, login to the web configurator. When the main screen appears, click once on **Network** > **Routing** >**OSPF** to open the following screen.

Figure 158 Network > Routing > OSPF



OSPF Router ID (IP Address): Default

Active	Route	Type	Metric(0-16777214)
☐	RIP	Type 1	
☐	Static Route	Type 1	

#	Area	Type	Authentication	

The following table describes the labels in this screen. See Section 13.4.2 on page 242 for more information as well.

Table 73 Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the ZyWALL uses in the OSPF AS. **Default** - the highest available IP address assigned to the interfaces is the ZyWALL's ID. **User Define** - enter the ID (in IP address format) in the field that appears when you select **User Define**.
Redistribute	

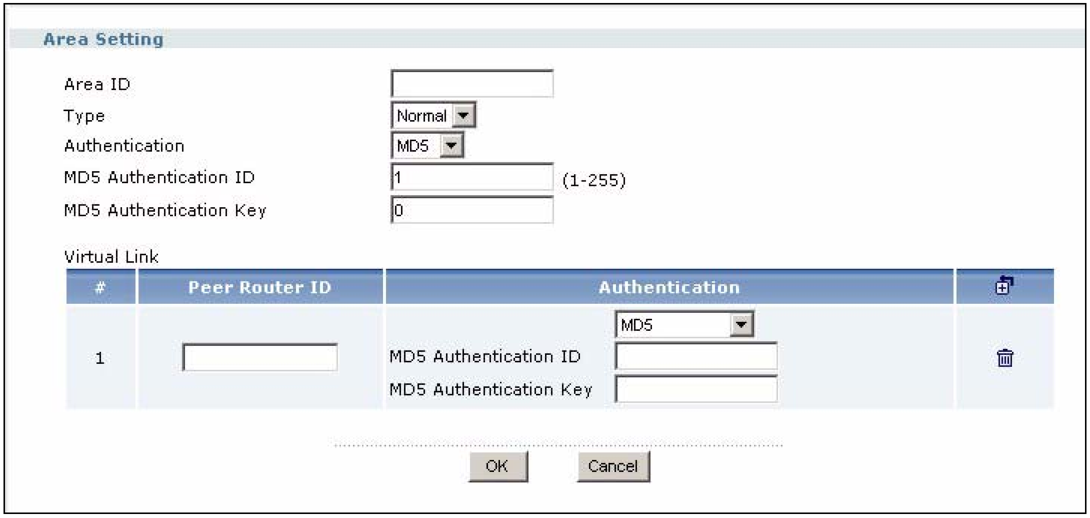
Table 73 Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Active	Select this check box to advertise routes that were learned from the indicated source. • If you select this for RIP, the ZyWALL advertises routes learned from RIP to **Normal** and **NSSA** areas but not to **Stub** areas. • If you select this for static routes, the ZyWALL advertises routes learned from static routes to all types of areas.
Route	This field displays other sources of routing information that the ZyWALL can advertise in the OSPF AS.
Type	Select how OSPF calculates the cost associated with routing information from the indicated source. Choices are: **Type 1** and **Type 2**. **Type 1** - cost = OSPF AS cost + external cost (**Metric**) **Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by the indicated source. The metric represents the “cost” of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Area	This section displays information about OSPF areas in the ZyWALL.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the **Type** field above.
Authentication	This field displays the default authentication method in the area.
Add icon	This column provides icons to add, edit, and remove areas. To add an area, click the **Add** icon at the top of the column. The **OSPF Area Add/Edit** screen appears. To edit an area, click the **Edit** icon next to the area. The **Area Add/Edit** screen appears. To delete an area, click on the **Remove** icon next to the area. The web configurator confirms that you want to delete the area before doing so.

13.4.2 OSPF Area Add/Edit

The **OSPF Area Add/Edit** screen allows you to create a new area or edit an existing one. To access this screen, go to the **OSPF** summary screen (see Section 13.4.1 on page 241), and click either the **Add** icon or an **Edit** icon.

Figure 159 Network > Routing > OSPF > Edit



Area Setting

Area ID

Type: Normal

Authentication: MD5

MD5 Authentication ID: 1 (1-255)

MD5 Authentication Key: 0

Virtual Link

#	Peer Router ID	Authentication
1		MD5 MD5 Authentication ID MD5 Authentication Key

The following table describes the labels in this screen.

Table 74 Network > Routing > OSPF > Edit

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	This field displays the type of area. **Normal** - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. **Stub** - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. **NSSA** - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	This field displays the default authentication method in the area. Choices are: **None**, **Text**, and **MD5**.
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the **Type** is **Normal**. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	Type the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	Select which authentication method to use in the virtual link. Choices are: **None**, **Text**, **MD5**, and **Same as Area**. In this case, **Same as Area** refers to the **Authentication** settings above.

Table 74 Network > Routing > OSPF > Edit (continued)

LABEL	DESCRIPTION
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Add icon	This column provides icons to add and remove virtual links. To add a virtual link, click the **Add** icon at the top of the column. A new record appears in the virtual link list. To delete a virtual link, click on the **Remove** icon next to the virtual link. The web configurator confirms that you want to delete the virtual link.

14

Zones

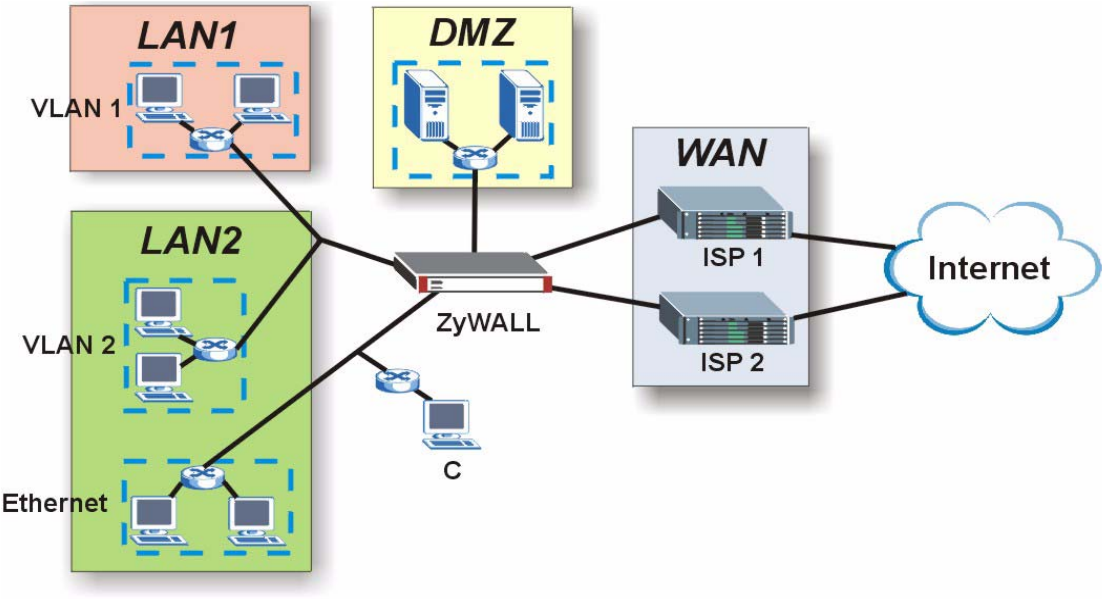
Set up zones to configure network security and network policies in the ZyWALL. See Section 5.4.7 on page 116 for related information on these screens.

14.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The ZyWALL uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, auxiliary interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 160 Example: Zones



14.1.1 Effect of Zones on Different Types of Traffic

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic--which are affected differently by zone-based security and policy settings.

Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 160 on page 245, traffic between VLAN 2 and the Ethernet is intra-zone traffic. In each zone, you can either allow or prohibit all intra-zone traffic. For example, in Figure 160 on page 245, you might allow intra-zone traffic in the LAN2 zone but prohibit it in the WAN zone. You can also set up firewall rules to control intra-zone traffic (for example, LAN2-to-LAN2), but many other types of zone-based security and policy settings do not affect intra-zone traffic.

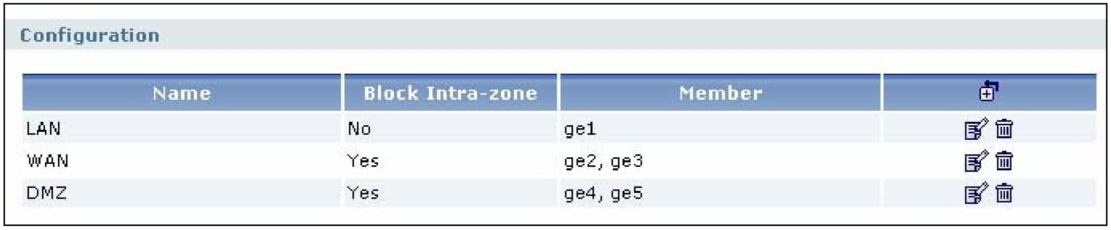
Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 160 on page 245, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 160 on page 245, traffic to or from computer **C** is extra-zone traffic. Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

14.2 Zone Summary

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Network** > **Zone**.

Figure 161 Network > Zone



Configuration

Name	Block Intra-zone	Member	
LAN	No	ge1	
WAN	Yes	ge2, ge3	
DMZ	Yes	ge4, ge5	

The following table describes the labels in this screen.

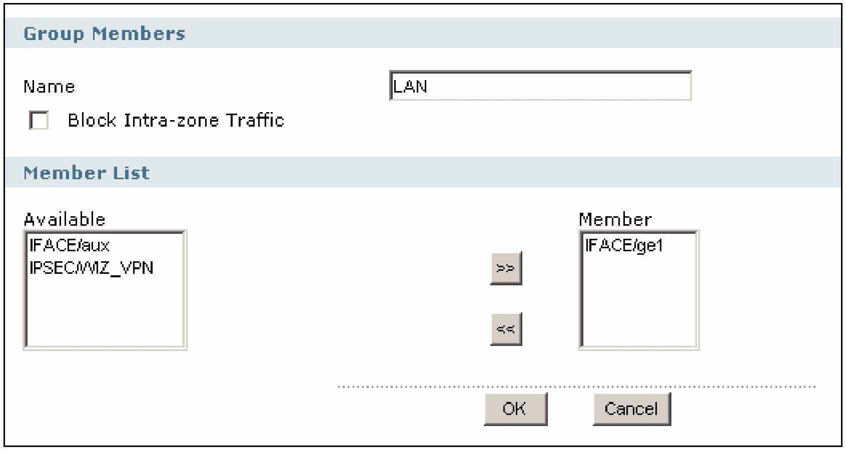
Table 75 Network > Zone

LABEL	DESCRIPTION
Name	This field displays the name of the zone.
Block Intra-zone	This field indicates whether or not the ZyWALL blocks network traffic between members in the zone.
Member	This field displays the names of the interfaces that belong to each zone.
Add icon	This column provides icons to add, edit, and remove zones. To add a zone, click the **Add** icon at the top of the column. The **Zone Add/Edit** screen appears. To edit a zone, click the **Edit** icon next to the zone. The **Zone Add/Edit** screen appears. To delete a zone, click the **Remove** icon next to the zone. The web configurator confirms that you want to delete the zone before doing so.

14.3 Zone Add/Edit

The **Zone Add/Edit** screen allows you to define a zone or edit an existing one. To access this screen, go to the **Zone** screen (see Section 14.2 on page 246), and click either the **Add** icon or an **Edit** icon.

Figure 162 Network > Zone > Edit



Name: LAN

☐ Block Intra-zone Traffic

Available: IFACE/aux, IPSEC/WIZ_VPN

Member: IFACE/ge1

The following table describes the labels in this screen.

Table 76 Network > Zone > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Block Intra-zone Traffic	Select this check box to block network traffic between members in the zone.
Member List	**Available** lists the interfaces that do not belong to any zone. The word in front of the name indicates whether this member is an interface or a VPN tunnel. **IFACE** - this member is an interface. **IPSEC** - this member is a VPN tunnel. Select any interfaces that you want to add to the zone you are editing, and click the right arrow button to add them. **Member** lists the interfaces that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.

15

DDNS

This chapter describes how to configure dynamic DNS (DDNS) services for the ZyWALL. First, it provides an overview, and then it introduces the screens. See Section 5.4.9 on page 117 for related information on these screens.

15.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

Before you can use Dynamic DNS services with the ZyWALL, you first need to set up a dynamic DNS account with www.dyndns.org. (This is the only DNS service provider the ZyWALL supports at the time of writing.) DynDNS offers several DNS services. Please see www. dyndns.org for more information about each of them. When registration is complete, DynDNS gives you a password or key.

You must go to DynDNS's Web site to set up a user account and a domain name before you can use the Dynamic DNS service with the ZyWALL.

After this, you configure the ZyWALL. Once the ZyWALL is configured, it automatically sends updated IP addresses to DynDNS, which helps redirect traffic accordingly.

15.1.1 DYNDNS Wildcard

Enable this feature to have *.yourhost.dyndns.org (for example, www.yourhost.dyndns.org) routed to the same IP address as yourhost.dyndns.org.

15.1.2 High Availability (HA)

The DDNS server maps a domain name to the IP address of one of the ZyWALL's WAN ports. If that WAN port loses its connection, high availability allows the ZyWALL to substitute the HA port's IP address in the domain name mapping.

15.1.3 Mail Exchanger

DynDNS can route e-mail for your domain name to a specified mail server. The server is called a mail exchanger. For example, if there is e-mail for john-doe@yourhost.dyndns.org, DynDNS routes the e-mail to the IP address you specify for the mail exchanger.

DynDNS can also provide an additional service, in which it holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. This service is called backup.

Please see www.dyndns.org for more information about mail exchangers and backup.

15.2 DDNS Screens

Each domain name requires information about the DynDNS services and DynDNS account, as well as how the ZyWALL updates the IP address.

The **DDNS Type** indicates which DynDNS service you are using. The ZyWALL supports three services: dynamic DNS, static DNS, and custom DNS. Please see www.dyndns.org for more information about each of these services.

The ZyWALL needs to know the **Username**, **Password**, and **Domain Name** for your DynDNS account. You can also use the **wildcard** check box to indicate whether or not the wildcard feature should be supported.

You must also specify an **IP Address Update Policy**. This policy controls how the ZyWALL determines the IP address that is mapped to your domain name in the DDNS server. There are three policies: **Interface**, **Auto**, and **Custom**.

- **Interface** - You specify which **WAN Interface** (WAN port's IP address) to use for the domain name, and you can also specify an alternative **HA Interface**, in case the WAN interface is not available.
- **Auto** - The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You might consider this if there are one or more NAT routers between the ZyWALL and the DDNS server.

The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.

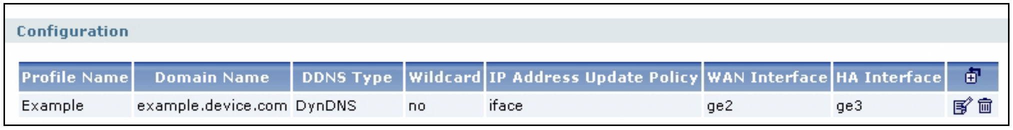
- **Custom** - If you have a static IP address, you can specify the **Custom IP** address to use for the domain name. The ZyWALL still sends the static IP address to the DDNS server.

15.3 DDNS Summary

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names.

To access this screen, login to the web configurator. When the main screen appears, click **Network** > **DDNS**. The following screen appears, providing a summary of the existing domain names.

Figure 163 Network > DDNS



Configuration

Profile Name	Domain Name	DDNS Type	Wildcard	IP Address Update Policy	WAN Interface	HA Interface	
Example	example.device.com	DynDNS	no	iface	ge2	ge3	

The following table describes the labels in this screen. See Section 15.4 on page 252 for more information as well.

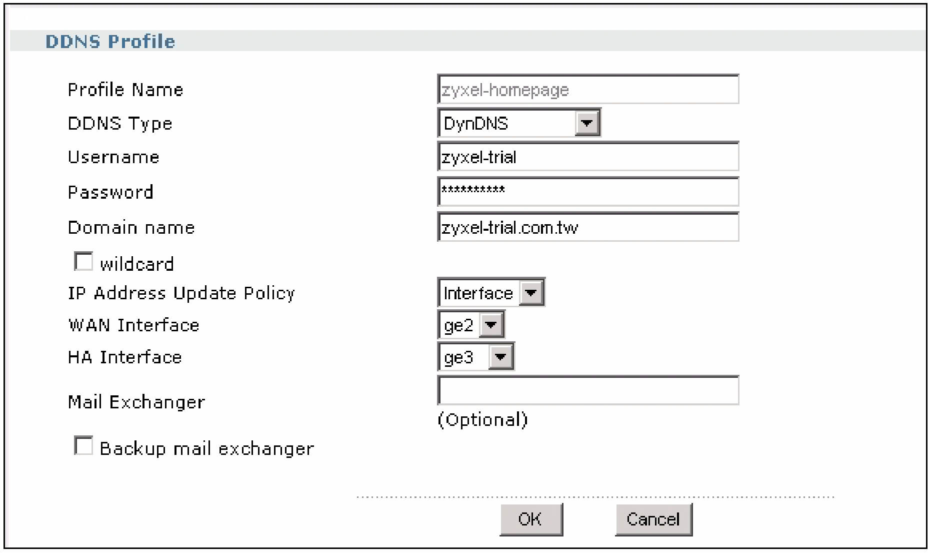
Table 77 Network > DDNS

LABEL	DESCRIPTION
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the ZyWALL can route.
DDNS Type	This field displays which DynDNS service you are using.
Wildcard	This field displays whether or not *.yourhost.dyndns.org (for example, www.yourhost.dyndns.org) is routed to the same IP address as yourhost.dyndns.org.
IP Address Update Policy	This field displays how the ZyWALL determines the IP address for the domain name. **iface** - The IP address comes from the specified **WAN Interface** and **HA Interface**. **auto** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. **custom** - The IP address is fixed. See Section 15.2 on page 250 for more information.
WAN Interface	This field applies when the **IP Address Update Policy** is **iface**. This field displays which interface is mapped to the domain name.
HA* Interface	High Availability maps an alternative WAN interface to the domain name when the **WAN interface** is not available. This field applies when the **IP Address Update Policy** is **iface**. This field displays which alternative interface is mapped to the domain name if the **WAN interface** is not available. If you are not using HA, the field says **none**.
Add icon	This column provides icons to add, edit, and remove domain names. To add a domain name, click the **Add** icon at the top of the column. The **DDNS Add/Edit** screen appears. To edit a domain name, click the **Edit** icon next to the domain name. The **DDNS Add/Edit** screen appears. To delete a domain name, click on the **Remove** icon next to the ISP account. The web configurator confirms that you want to delete the account before doing so.

15.4 Dynamic DNS Add/Edit

The **DDNS Add/Edit** screen allows you to add a domain name to the ZyWALL or to edit the configuration of an existing domain name. To access this screen, click **Network** > **DDNS**, and click either the **Add** icon or an **Edit** icon.

Figure 164 Network > DDNS > Edit



DDNS Profile

Profile Name: zyxel-homepage
DDNS Type: DynDNS
Username: zyxel-trial
Password: **********
Domain name: zyxel-trial.com.tw
☐ wildcard
IP Address Update Policy: Interface
WAN Interface: ge2
HA Interface: ge3
Mail Exchanger: (Optional)
☐ Backup mail exchanger

The following table describes the labels in this screen.

Table 78 Network > DDNS > Edit

LABEL	DESCRIPTION
Profile Name	Type a descriptive name for this DDNS entry in the ZyWALL. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
DDNS Type	Select the type of DynDNS service you are using. See http://www.dyndns.com for more information about each one.
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.
Password	Type the password provided by DynDNS. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Domain name	Type the domain name you registered. You can use up to 255 characters.
Wildcard	Select this if *.yourhost.dyndns.org (for example, www.yourhost.dyndns.org) should be routed to the same IP address as yourhost.dyndns.org.
IP Address Update Policy	Select how the ZyWALL determines the IP address for the domain name. **Interface** - The IP address comes from the specified **WAN Interface** and **HA Interface**. **Auto** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ZyWALL and the DDNS server. **Custom** - The IP address is fixed. See Section 15.2 on page 250 for more information.
WAN Interface	This field is only available when the **IP Address Update Policy** is **Interface**. Select the interface to use for updating the IP address mapped to the domain name.

Table 78 Network > DDNS > Edit (continued)

LABEL	DESCRIPTION
HA Interface	This field is only available when the **IP Address Update Policy** is **Interface**. Select the alternative WAN interface to map to the domain name when the **WAN interface** is not available. If you do not want to use HA, select **none**.
Custom IP	This field is only available when the **IP Address Update Policy** is **Custom**. Type the IP address to use for the domain name.
Mail Exchanger	Type the name of your mail server here, if DynDNS also routes e-mail to this domain name. This field should be left blank if DynDNS does not.
Backup mail exchanger	Select this check box if you are using DynDNS's backup service for e-mail. Please see www.dyndns.org for more information about this service.

16

Virtual Servers

This chapter describes how to set up, manage, and remove virtual servers. First, it provides an overview of virtual servers, and, then, it introduces the virtual server screens and commands. See Section 5.4.18 on page 121 for related information on these screens.

16.1 Virtual Server Overview

Virtual server is also known as port forwarding or port translation.

The virtual server changes the destination address of packets. This is also known as Destination NAT (DNAT).

Virtual servers are computers on a private network behind the ZyWALL that you want to make available outside the private network. If the ZyWALL has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

In the ZyWALL, you set up a virtual server for each forwarding rule. The first part of the virtual server defines the conditions required to forward the packet.

- **Original IP** - the original destination address; it can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface; a specific IP address; or a HOST address object. (See Chapter 35 on page 515.)
- **Protocol Type** - the protocol [TCP, UDP, or both (**Any**)] used by the service requesting the connection.
- **Original Port(s)** - the original destination port or range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service.

The second part of the virtual server controls where the packet is forwarded if the conditions are satisfied.

- **Mapped IP** - the translated destination address.
- **Mapped Port(s)** - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

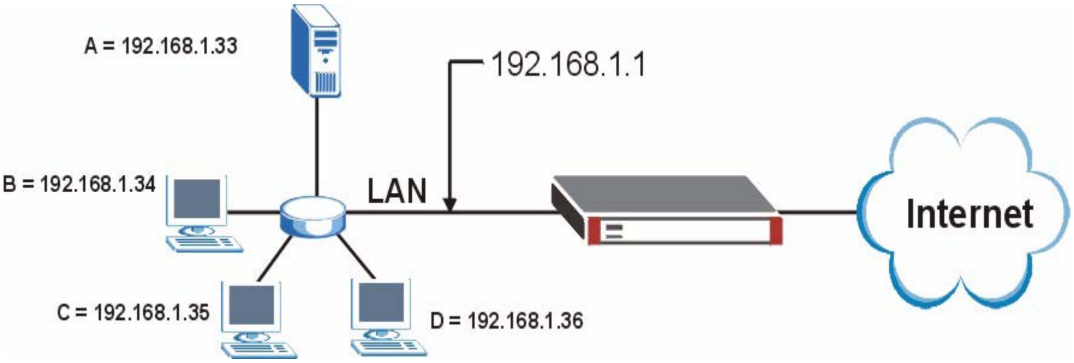
The ZyWALL checks virtual servers before it applies to-ZyWALL firewall rules, so to-ZyWALL firewall rules do not apply to traffic that is forwarded by virtual servers. The ZyWALL still checks regular (through-ZyWALL) firewall rules according to the source IP address and mapped IP address.

Some common port numbers are listed in Appendix C on page 703.

16.2 Virtual Server Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 165 Multiple Servers Behind NAT Example



16.3 Virtual Server Screens

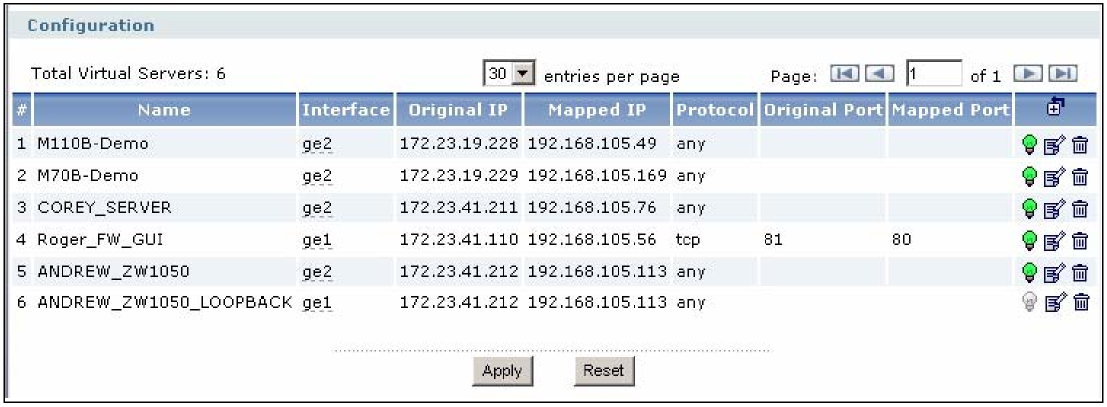
The **Virtual Server** summary screen provides a summary of all virtual servers and their configuration, and the **Virtual Server Add/Edit** screen lets you configure a virtual server.

16.4 Virtual Server Summary Screen

The **Virtual Server** summary screen provides a summary of all virtual servers and their configuration. In addition, this screen allows you to create new virtual servers and edit and delete existing virtual servers.

To access this screen, login to the web configurator. When the main screen appears, click **Network** > **Virtual Server**. The following screen appears, providing a summary of the existing virtual servers.

Figure 166 Network > Virtual Server



Configuration

Total Virtual Servers: 6

#	Name	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
1	M110B-Demo	ge2	172.23.19.228	192.168.105.49	any		
2	M70B-Demo	ge2	172.23.19.229	192.168.105.169	any		
3	COREY_SERVER	ge2	172.23.41.211	192.168.105.76	any		
4	Roger_FW_GUI	ge1	172.23.41.110	192.168.105.56	tcp	81	80
5	ANDREW_ZW1050	ge2	172.23.41.212	192.168.105.113	any		
6	ANDREW_ZW1050_LOOPBACK	ge1	172.23.41.212	192.168.105.113	any		

The following table describes the labels in this screen. See Section 16.4.1 on page 258 below for more information as well.

Table 79 Network > Virtual Server

LABEL	DESCRIPTION
Total Virtual Servers	This is how many virtual server entries are configured in the ZyWALL.
entries per page	Select how many virtual server entries to display per page in the screen.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific virtual server.
Name	This field displays the name of the virtual server.
Interface	This field displays the interface on which packets for the virtual server were received.
Original IP	This field displays the original destination IP address (or address object) of packets for the virtual server. It displays **any** if there is no restriction on the original destination IP address.
Mapped IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this virtual server. It displays **any** if there is no restriction on the services.
Original Port	This field displays the original destination port(s) of packets for the virtual server. This field is blank if there is no restriction on the original destination port.
Mapped Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Add icon	This column provides icons to add, edit, and remove virtual servers. In addition, you can activate and deactivate virtual servers. To add a virtual server, click the **Add** icon at the top of the column. The **Virtual Server Add/Edit** screen appears. To activate / deactivate a virtual server, click the **Active** icon next to the virtual server. To edit a virtual server, click the **Edit** icon next to the virtual server. The **Virtual Server Add/Edit** screen appears. To delete a virtual server, click on the **Remove** icon next to the virtual server. The web configurator confirms that you want to delete it before doing so.

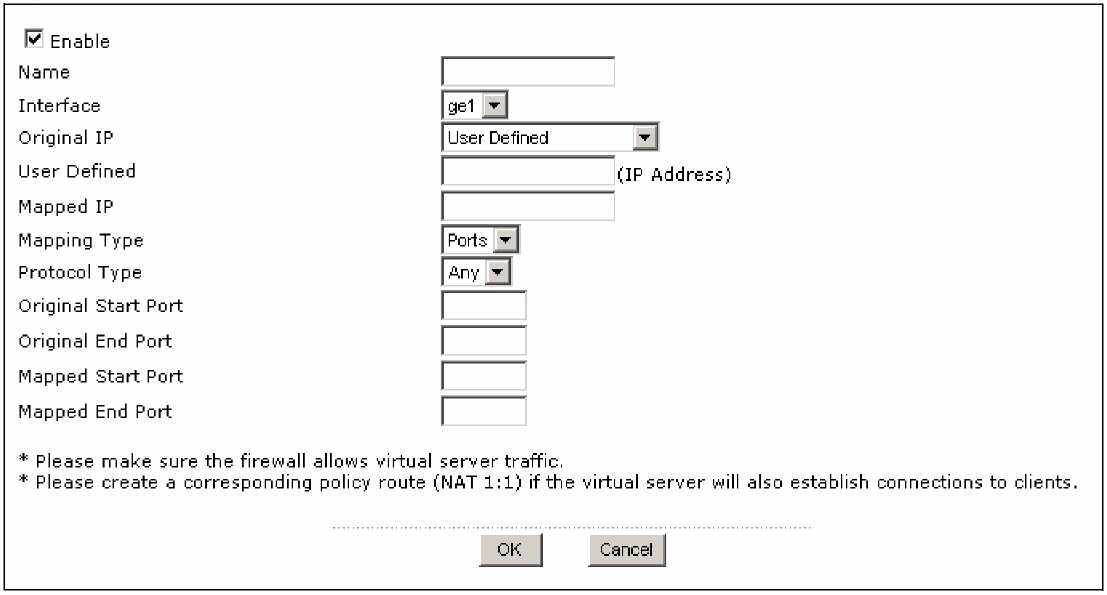
16.4.1 Virtual Server Add/Edit

The **Virtual Server Add/Edit** screen lets you create new virtual servers and edit existing ones. To open this window, open the **Virtual Server** summary screen. (See Section 16.4 on page 256.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

If the virtual server will send traffic to the clients, you need to create a corresponding policy route. This is called NAT 1:1.

See Section 6.6 on page 147 for an example of NAT 1:1.

Figure 167 Network > Virtual Server > Edit



☑ Enable
Name
Interface: ge1
Original IP: User Defined
User Defined (IP Address)
Mapped IP
Mapping Type: Ports
Protocol Type: Any
Original Start Port
Original End Port
Mapped Start Port
Mapped End Port

* Please make sure the firewall allows virtual server traffic.
* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish connections to clients.

The following table describes the labels in this screen.

Table 80 Network > Virtual Server > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the virtual server on or off.
Name	Type in the name of the virtual server. The name is used to refer to the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which packets for the virtual server must be received.
Original IP	Use the drop-down list box to indicate which destination IP address this virtual server supports. Choices are: **Any** - this virtual server supports the IP address of the selected interface. **User Defined** - this virtual server supports a specific IP address, specified in the **User Defined** field. HOST address - the drop-down box lists all the HOST address objects in the ZyWALL. If you select one of them, this virtual server supports the IP address specified by the address object. Select **Create Object** to configure a new IP address object.

Table 80 Network > Virtual Server > Edit (continued)

LABEL	DESCRIPTION
User Defined	This field is available if **Original IP** is **User Defined**. Type the destination IP address that this virtual server supports.
Mapped IP	Type the translated destination IP address, if this virtual server forwards the packet.
Mapping Type	Use the drop-down list box to select how many original destination ports this virtual server supports for the selected destination IP address (**Original IP**). Choices are: **Any** - this virtual server supports all the destination ports. **Port** - this virtual server supports one destination port. **Ports** - this virtual server supports a range of destination ports.
Protocol Type	This field is available if **Mapping Type** is **Port** or **Ports**. Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **Any**.
Original Port	This field is available if **Mapping Type** is **Port**. Enter the original destination port this virtual server supports.
Mapped Port	This field is available if **Mapping Type** is **Port**. Enter the translated destination port if this virtual server forwards the packet.
Original Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of original destination ports this virtual server supports.
Original End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of original destination ports this virtual server supports.
Mapped Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of translated destination ports if this virtual server forwards the packet.
Mapped End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of translated destination ports if this virtual server forwards the packet.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to return to the **Virtual Server** summary screen without creating the virtual server (if it is new) or saving any changes (if it already exists).

17

HTTP Redirect

This chapter shows you how to configure HTTP redirection on your ZyWALL. See Section 5.4.19 on page 121 for related information on these screens.

17.1 HTTP Redirect Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ZyWALL) to a web proxy server.

17.1.1 Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

17.2 HTTP Redirect, Firewall and Policy Route

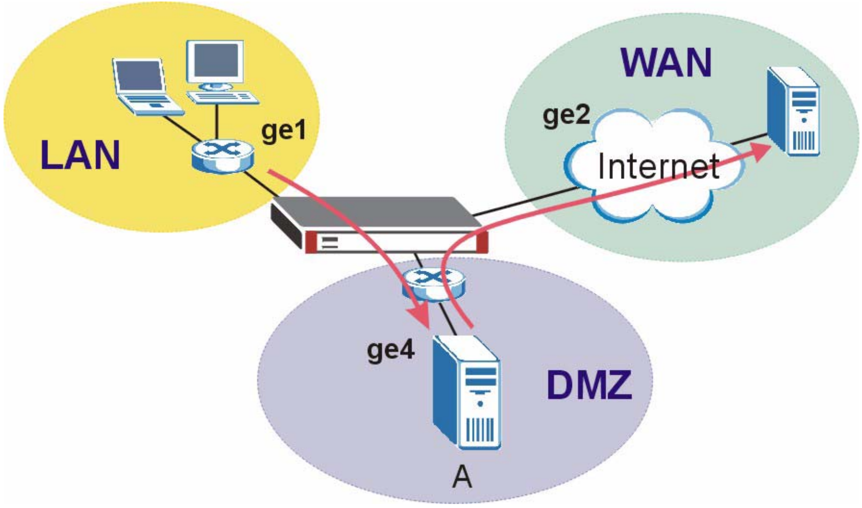
With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Firewall
2. Application Patrol
3. HTTP Redirect
4. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the ZyWALL checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no firewall rule(s) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet.

Figure 168 HTTP Redirect Example



In the example, proxy server **A** is connected to **ge4** in the DMZ zone. When a client connected to **ge1** wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

To make this example work, make sure you have the following settings.

For HTTP traffic between **ge1** and **ge4**:

- a from LAN to WAN through-ZyWALL rule (default) to allow HTTP request from **ge1** to **ge4**. Responses to this request are allowed automatically.
- a application patrol rule to allow HTTP traffic between **ge1** and **ge4**.
- a HTTP redirect rule to forward HTTP traffic from **ge1** to proxy server **A**.

For HTTP traffic between **ge4** and **ge2**:

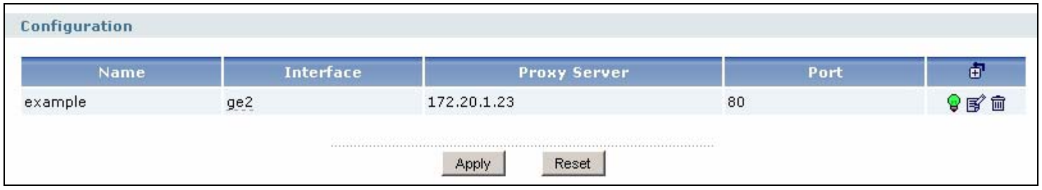
- a from DMZ to WAN through-ZyWALL rule (default) to allow HTTP request from **ge4** to **ge2**. Responses to this request are allowed automatically.
- a application patrol rule to allow HTTP traffic between **ge4** and **ge2**.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

17.3 Configuring HTTP Redirect

To configure redirection of a HTTP request to a proxy server, click **Network** > **HTTP Redirect**. This screen displays the summary of the HTTP redirect rules.

You can configure up to one HTTP redirect rule for each (incoming) interface.

Figure 169 Network > HTTP Redirect



Name	Interface	Proxy Server	Port
example	ge2	172.20.1.23	80

The following table describes the labels in this screen.

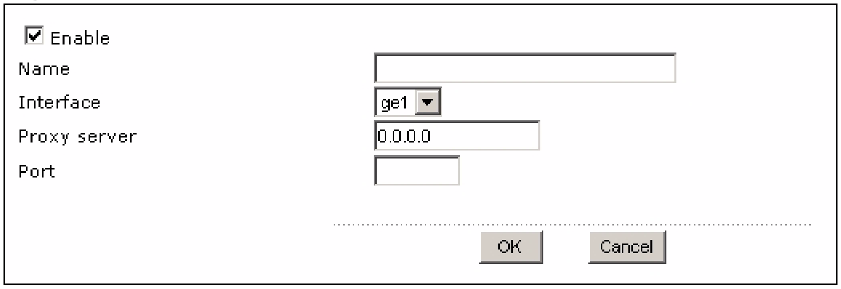
Table 81 Network > HTTP Redirect

LABEL	DESCRIPTION
Name	This is the descriptive name (up to 31 printable characters) of a rule.
Interface	This is the interface on which the request must be received.
Proxy Server	This is the IP address of the proxy server.
Port	This is the service port number used by the proxy server.
Add icon	Click the **Add** icon in the heading row to add a new entry. The **Active** icon displays whether the rule is enabled or not. Click the **Active** icon to activate or deactivate the rule. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the rule on the ZyWALL. Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

17.4 HTTP Redirect Edit

Click **Network** > **HTTP Redirect** to open the **HTTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **HTTP Redirect Edit** screen where you can configure the rule.

Figure 170 Network > HTTP Redirect > Edit



☑ Enable

Name	
Interface	ge1
Proxy server	0.0.0.0
Port	

The following table describes the labels in this screen.

Table 82 Network > HTTP Redirect > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the HTTP redirect rule on or off.
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 82 Network > HTTP Redirect > Edit (continued)

LABEL	DESCRIPTION
Interface	Select the interface on which the HTTP request must be received for the ZyWALL to forward it to the specified proxy server.
Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number that the proxy server uses.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

18

ALG

This chapter covers how to use the ZyWALL's ALG feature to allow certain applications to pass through the ZyWALL. See Section 5.4.20 on page 122 for related information on these screens.

18.1 ALG Introduction

The ZyWALL can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has VoIP pass through enabled, the ZyWALL translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The ZyWALL only needs to use the ALG feature for traffic that goes through the ZyWALL's NAT. The firewall allows related sessions. The firewall allows or blocks peer to peer traffic based on the firewall rules.

You do not need to use STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) for VoIP devices behind the ZyWALL when you enable the SIP ALG.

18.1.1 Application Layer Gateway (ALG) and NAT

The ZyWALL dynamically creates an implicit NAT session for the application's traffic from the WAN to the LAN. The ALG on the ZyWALL supports all of the ZyWALL's NAT mapping types.

18.1.2 ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The ZyWALL does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

18.1.3 FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. The FTP ALG allows TCP packets with a port 21 destination to pass through. If the FTP server is located on the LAN, you must also configure NAT port forwarding and firewall rules if you want to allow access to the server from the WAN.

18.1.4 H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

18.1.5 RTP

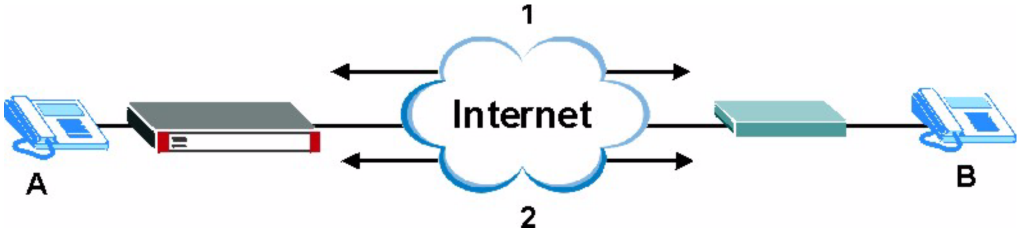
When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

18.1.5.1 H.323 ALG Details

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyWALL routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The ZyWALL allows H.323 audio connections.
- The ZyWALL can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 171 H.323 ALG Example



18.1.6 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

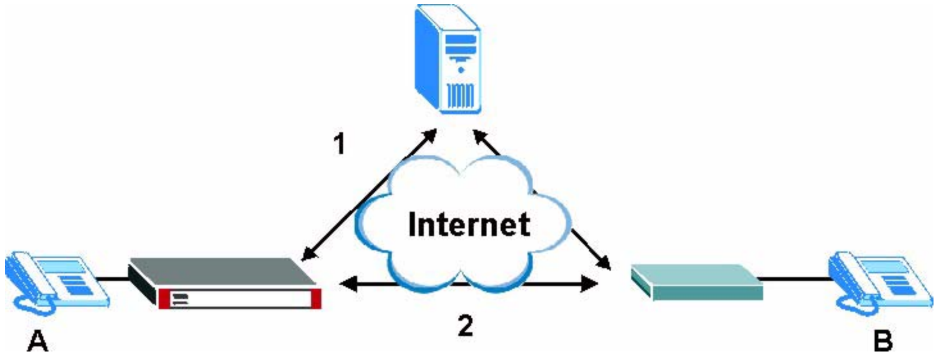
SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

18.1.6.1 SIP ALG Details

- SIP clients can be connected to the LAN or DMZ. A SIP server must be on the WAN.
- Using the SIP ALG allows you to use bandwidth management on SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the ZyWALL routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The firewall (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The ZyWALL allows SIP audio connections.

The following example shows SIP signaling (1) and audio (2) sessions between SIP clients A and B and the SIP server.

Figure 172 SIP ALG Example



18.1.6.2 SIP Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL.

If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout, the ZyWALL SIP ALG deletes the signaling session after the timeout period.

18.2 Peer-to-Peer Calls and the ZyWALL

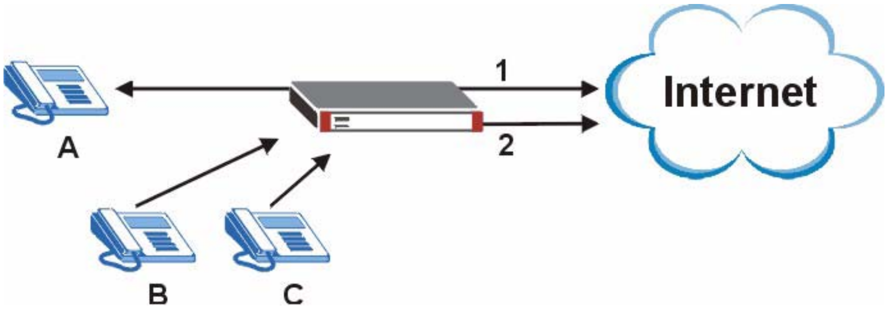
The ZyWALL ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the firewall and virtual server (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

18.2.1 VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the firewall and virtual server (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the firewall and virtual server to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 173 VoIP Calls from the WAN with Multiple Outgoing Calls

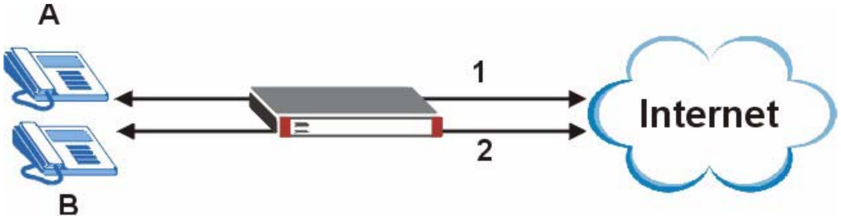


18.2.2 VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and virtual server (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure firewall and virtual server rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

Figure 174 VoIP with Multiple WAN IP Addresses

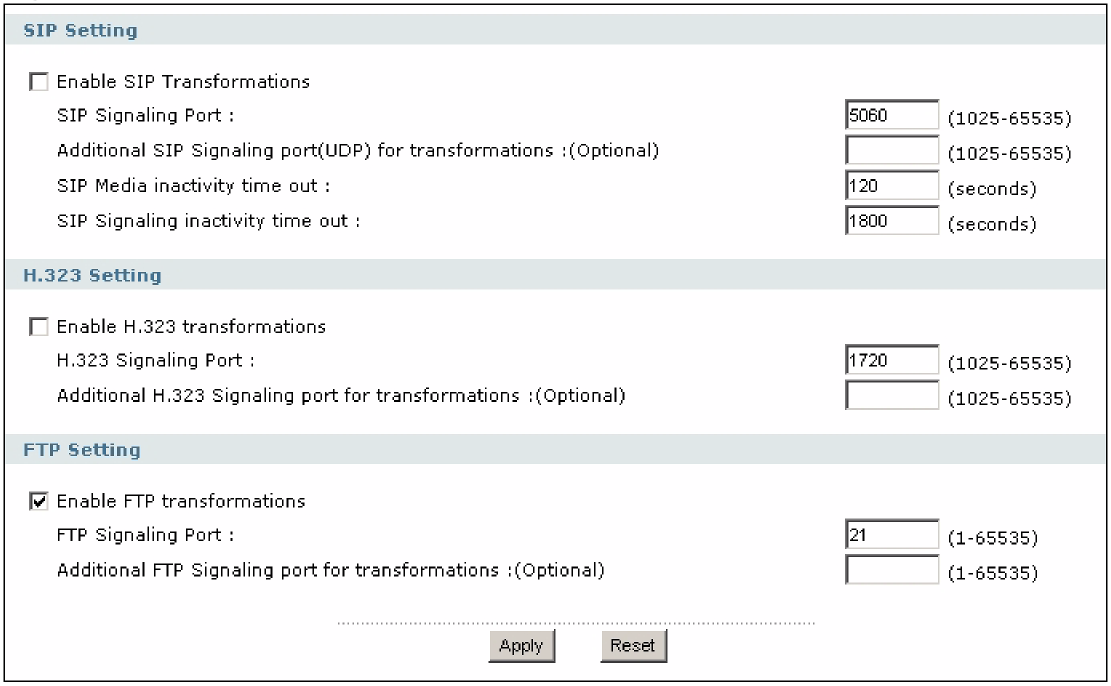


18.3 ALG Screen

Click **Network** > **ALG** to open the **ALG** screen. Use this screen to turn ALGs off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

If the ZyWALL provides an ALG for a service, you must enable the ALG in order to perform bandwidth management on that service's traffic.

Figure 175 Network > ALG



SIP Setting

☐ Enable SIP Transformations

SIP Signaling Port : 5060 (1025-65535)

Additional SIP Signaling port(UDP) for transformations :(Optional) (1025-65535)

SIP Media inactivity time out : 120 (seconds)

SIP Signaling inactivity time out : 1800 (seconds)

H.323 Setting

☐ Enable H.323 transformations

H.323 Signaling Port : 1720 (1025-65535)

Additional H.323 Signaling port for transformations :(Optional) (1025-65535)

FTP Setting

☑ Enable FTP transformations

FTP Signaling Port : 21 (1-65535)

Additional FTP Signaling port for transformations :(Optional) (1-65535)

The following table describes the labels in this screen.

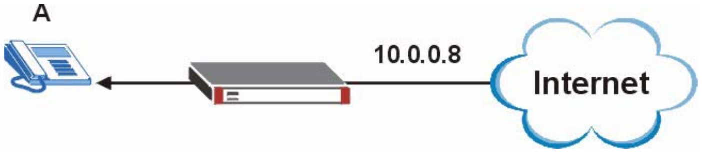
Table 83 Network > ALG

LABEL	DESCRIPTION
Enable SIP Transformations	SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol. Turn on the SIP ALG to allow SIP sessions to pass through the ZyWALL. Using the SIP ALG allows you to use bandwidth management on SIP traffic.
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
Additional SIP Signaling port (UDP) for transformations	If you are also using SIP on an additional UDP port number, enter it here.
SIP Media inactivity time out	Use this field to set how many seconds (1~86400) the ZyWALL will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the ZyWALL deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.
SIP Signaling inactivity time out	Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL. If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout, the ZyWALL deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).
Enable H.323 transformations	H.323 is a protocol used for audio communications over networks. Select this check box to turn on the H.323 ALG to allow H.323 sessions to pass through the ZyWALL. Using the H.323 ALG allows you to use bandwidth management on H.323 traffic.
H.323 Signaling Port	If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here.
Additional H.323 Signaling port for transformations	If you are also using H.323 on an additional TCP port number, enter it here.
Enable FTP Transformations	Select this check box to allow FTP sessions to pass through the ZyWALL. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail. Using the FTP ALG allows you to use bandwidth management on FTP traffic.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.
Additional FTP Signaling port for transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.4 WAN to LAN SIP Peer-to-peer Calls Example

This example shows how to configure firewall and virtual server (port forwarding) rules to allow H.323 calls to come in through WAN IP address 10.0.0.8 to computer A at IP address 192.168.1.56 on the LAN.

Figure 176 WAN to LAN H.323 Peer-to-peer Calls Example

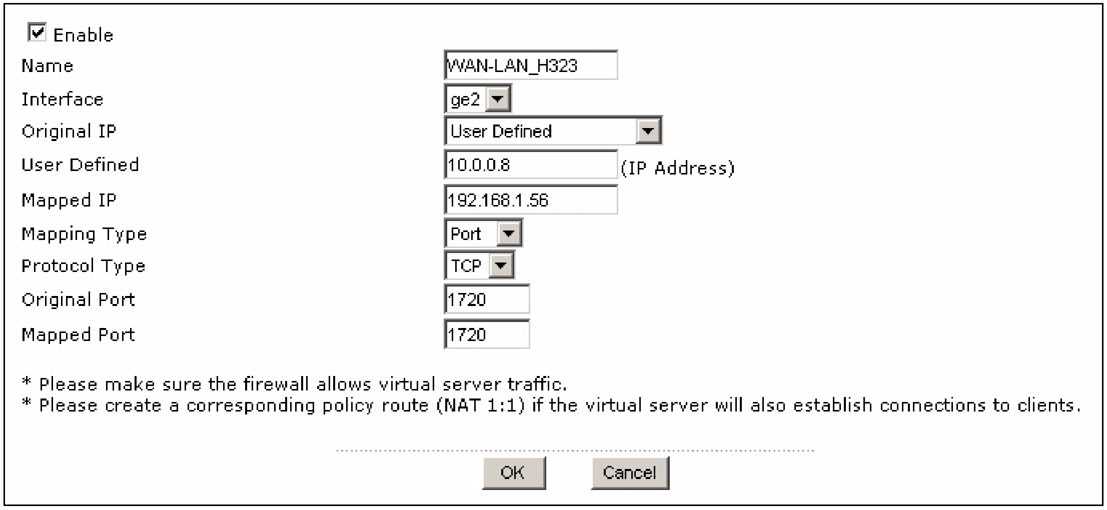


Configure the virtual server policy first to forward H.323 (TCP port 1720) traffic received on the ZyWALL’s 10.0.0.8 WAN IP address to LAN IP address 192.168.1.56.

1 Click **Network** > **Virtual Server** > **Add.**

2 Configure the screen as follows and click **OK**.

Figure 177 Network > Virtual Server > Add



☑ Enable

Name	WAN-LAN_H323
Interface	ge2
Original IP	User Defined
User Defined	10.0.0.8 (IP Address)
Mapped IP	192.168.1.56
Mapping Type	Port
Protocol Type	TCP
Original Port	1720
Mapped Port	1720

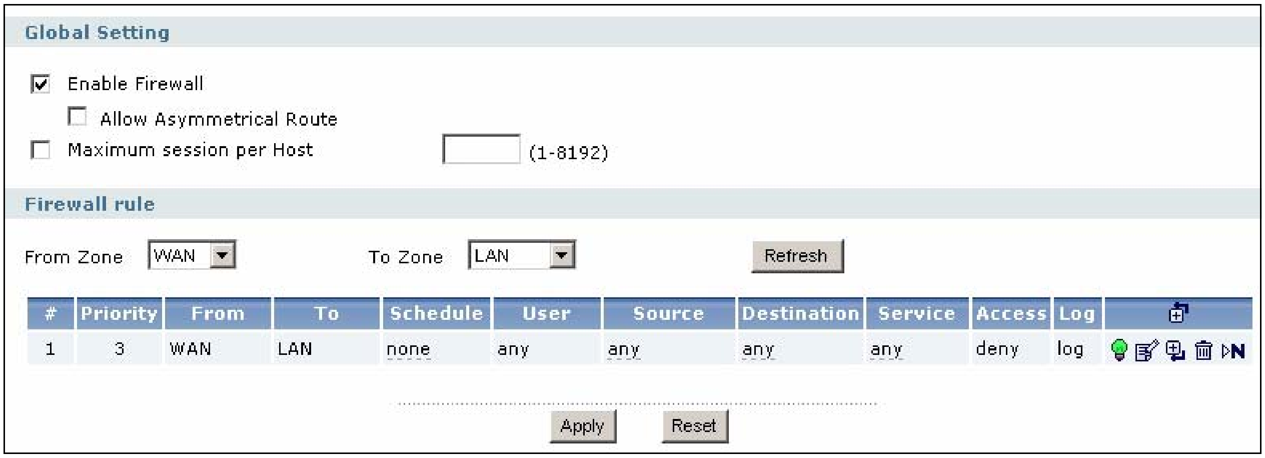
* Please make sure the firewall allows virtual server traffic.
* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish connections to clients.

Now configure a firewall rule to allow H.323 (TCP port 1720) traffic received on the WAN_IP-for-H323 IP address to go to LAN IP address 192.168.1.56.

3 Click **Firewall**. In **From Zone**, select **WAN**; in **To Zone**, select **LAN.**

4 The default rule for WAN-to-LAN traffic drops all traffic. You want to allow SIP access through IP address 10.0.0.8, so add a rule before the default rule. Click the **Add** icon at the top of the column.

Figure 178 Firewall > WAN to LAN



Global Setting

☑ Enable Firewall

☐ Allow Asymmetrical Route

☐ Maximum session per Host (1-8192)

Firewall rule

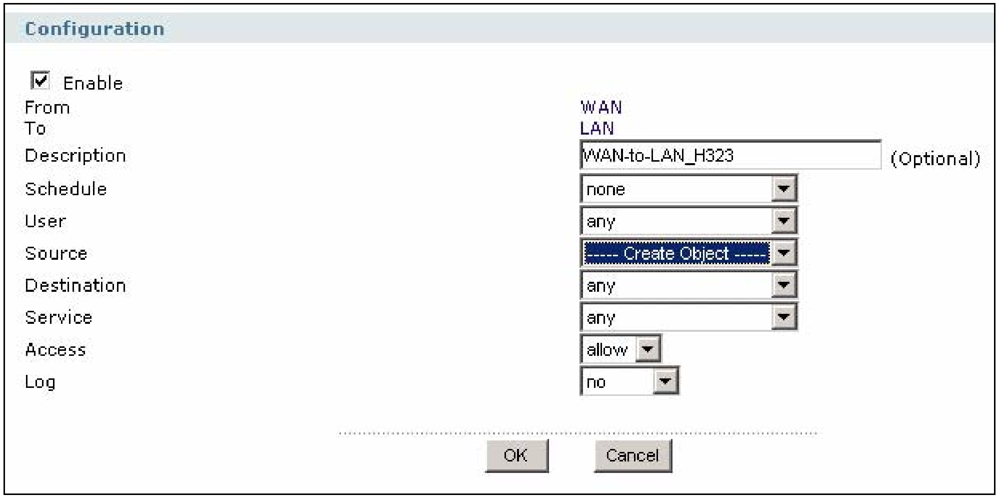
From Zone: WAN

To Zone: LAN

#	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1	3	WAN	LAN	none	any	any	any	any	deny	log

5 Configure the screen as follows. For the **Destination**, select **Create Object**.

Figure 179 Firewall > WAN > LAN > Add



Configuration

☑ Enable

From: WAN

To: LAN

Description: WAN-to-LAN_H323 (Optional)

Schedule: none

User: any

Source: ----- Create Object -----

Destination: any

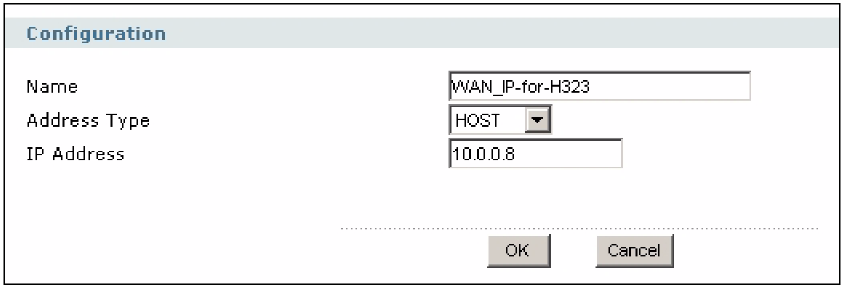
Service: any

Access: allow

Log: no

6 Configure an address object for the ZyWALL’s 10.0.0.8 WAN IP address as follows and click **OK**.

Figure 180 Object > Address > Add



Configuration

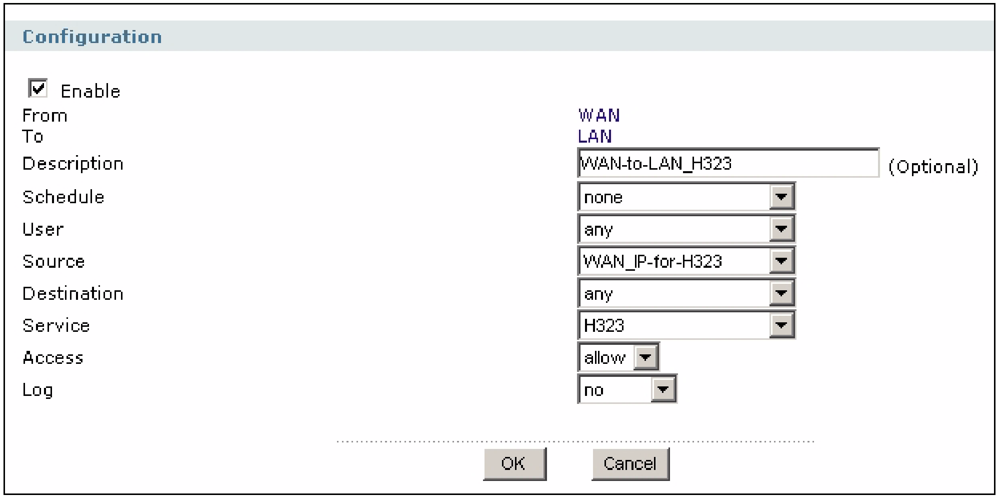
Name: WAN_IP-for-H323

Address Type: HOST

IP Address: 10.0.0.8

7 Finish configuring the screen as follows and click **OK**.

Figure 181 Firewall > WAN > LAN > Add



☑ Enable

From	WAN
To	LAN
Description	WAN-to-LAN_H323 (Optional)
Schedule	none
User	any
Source	WAN_IP-for-H323
Destination	any
Service	H323
Access	allow
Log	no

PART III

Firewall and VPN

Firewall (277)
IPSec VPN (291)
SSL VPN (323)
SSL User Screens (331)
SSL User Application Screens (337)
SSL User File Sharing Screens (339)
L2TP VPN (345)
L2TP VPN Example (351)

19

Firewall

This chapter introduces the ZyWALL's firewall and shows you how to configure your ZyWALL's firewall. See Section 5.4.12 on page 118 for related information on these screens.

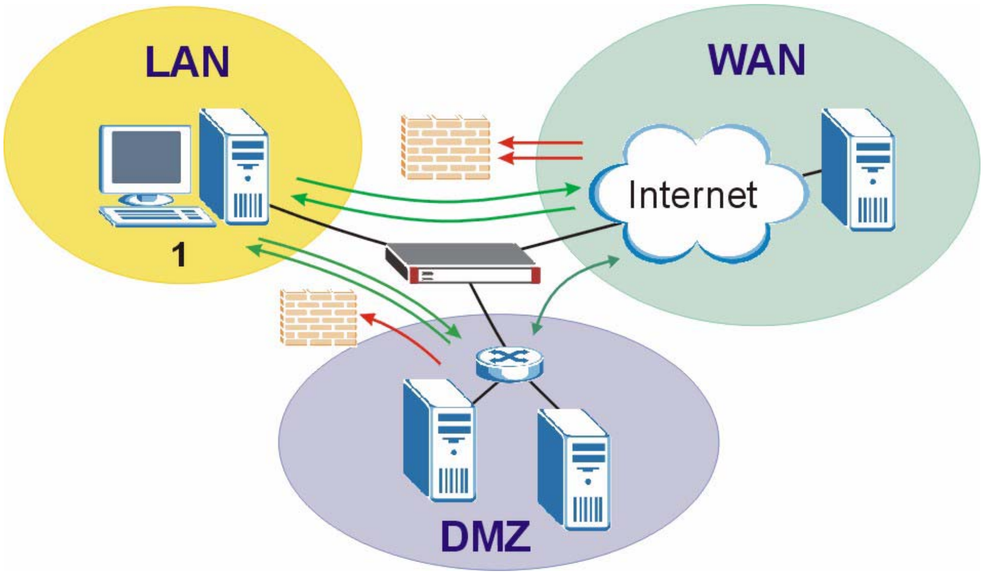
19.1 Firewall Overview

The ZyWALL's firewall is a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

A zone is a group of interfaces or VPN tunnels. Group the ZyWALL's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

The following figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN zone is blocked. Communications between the WAN and the DMZ zones are allowed. The firewall allows VPN traffic between any of the networks.

Figure 182 Default Firewall Action



Your customized rules take precedence and override the ZyWALL's default settings. The ZyWALL checks the schedule, user name (user's login name on the ZyWALL), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL takes the action specified in the rule.

For example, if you want to allow a specific user from any computer to access one zone by logging in to the ZyWALL, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ZyWALL and will be disabled after the user logs out of the ZyWALL.

19.2 Firewall Rules

Firewall rules are grouped based on the direction of travel of packets to which they apply.

The LAN, WAN, and DMZ zones are default zones.Refer to Chapter 14 on page 245 for more information on zones.

If you create a new zone, there is no default firewall rule for it and any packets sent to or from the new zone are allowed.

19.2.1 Rule Directions

The following table shows you the default firewall rules that inspect packets going through the ZyWALL.

The ZyWALL checks the firewall rules before the application patrol rules for traffic going through the ZyWALL.

If you want to use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

You can use the firewall to block a service with a static port number. To block a service using a flexible/dynamic port number by inspecting the service's packets, you need to use application patrol. See the chapter about application patrol for more information.

The following table explains the default firewall rules for traffic going through the ZyWALL. See Section 19.2.1.2 on page 279 for details on the firewall rules for traffic going to the ZyWALL itself.

Table 84 Default Firewall Rules

FROM ZONE TO ZONE	STATEFUL PACKET INSPECTION
From LAN to LAN	Traffic between interfaces in the LAN is allowed.
From LAN to WAN	Traffic from the LAN to the WAN is allowed.
From LAN to DMZ	Traffic from the LAN to the DMZ is allowed.
From WAN to LAN	Traffic from the WAN to the LAN is dropped.
From WAN to WAN	Traffic between interfaces in the WAN is dropped.
From WAN to DMZ	Traffic from the WAN to the DMZ is allowed.
From WAN to ZyWALL	Traffic from the WAN to the ZyWALL itself is dropped except for the traffic types described in Section 19.2.1.2 on page 279.
From DMZ to LAN	Traffic from the DMZ to the LAN is dropped.
From DMZ to WAN	Traffic from the DMZ to the WAN is dropped.
From DMZ to DMZ	Traffic between interfaces in the DMZ is dropped.

If you enable intra-zone traffic blocking (see the chapter about zones), the firewall automatically creates (implicit) rules to deny packet passage between the interfaces in the specified zone.

You also need to configure virtual servers (NAT port forwarding) to allow computers on the WAN to access devices on the LAN. See Chapter 16 on page 255 for more information.

19.2.1.1 Global Firewall Rules

If an interface or VPN tunnel is not included in a zone, only the global firewall rules (with **from any to any** direction) apply to traffic going to and from that interface.

19.2.1.2 To-ZyWALL Rules

Rules with **ZyWALL** as the **To Zone** apply to traffic going to the ZyWALL itself. By default, the firewall allows any computer from the LAN zone to access or manage the ZyWALL. By default, the ZyWALL drops most packets from the WAN or DMZ zone to the ZyWALL itself, except for VRRP traffic for Device HA and ESP/AH/IKE/NATT/HTTPS services for VPN tunnels, and generates a log.

When you configure a to-ZyWALL rule for packets destined for the ZyWALL itself, make sure it does not conflict with your service control rule. See Chapter 43 on page 575 for more information about service control (remote management).

The ZyWALL checks the firewall rules before the service control rules for traffic destined for the ZyWALL.

You can configure a to-ZyWALL firewall rule (with **From Any To ZyWALL** direction) for traffic from an interface which is not in a zone.

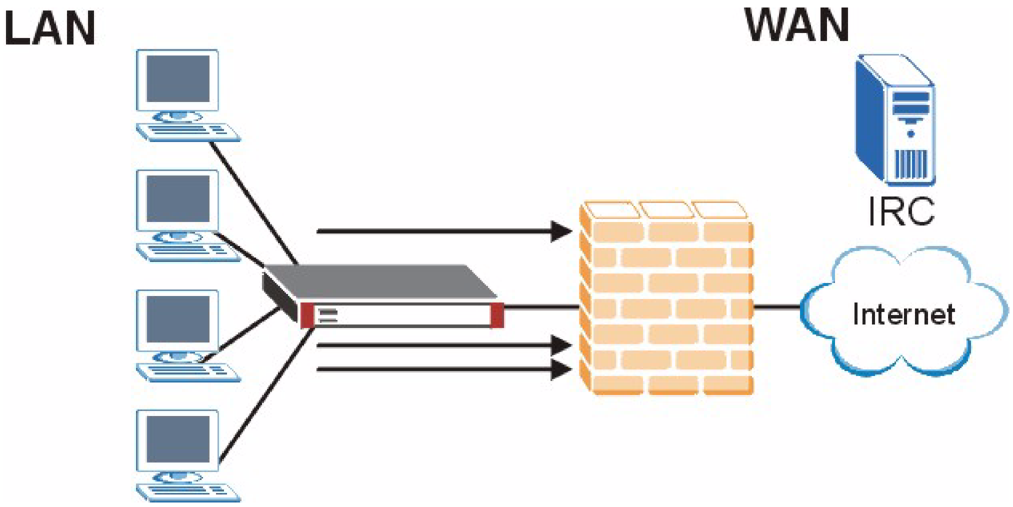
19.2.2 Firewall and VPN Traffic

After you create a VPN tunnel and apply it to a zone, you can set the firewall rules applied to VPN traffic. If you add a VPN tunnel to an existing zone (the LAN zone for example), you can configure a new LAN to LAN firewall rule or use intra-zone traffic blocking to allow or block VPN traffic transmitting between the VPN tunnel and other interfaces in the LAN zone. If you add the VPN tunnel to a new zone (the VPN zone for example), you can configure rules for VPN traffic between the VPN zone and other zones or **From VPN To-ZyWALL** rules for VPN traffic destined for the ZyWALL.

19.3 Firewall Rule Example Applications

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

Figure 183 Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 85 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATIO N	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
Default	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all traffic from the LAN to go to the WAN.

The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the ZyWALL forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN rule that allows IRC traffic from any computer through which the CEO logs into the ZyWALL with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

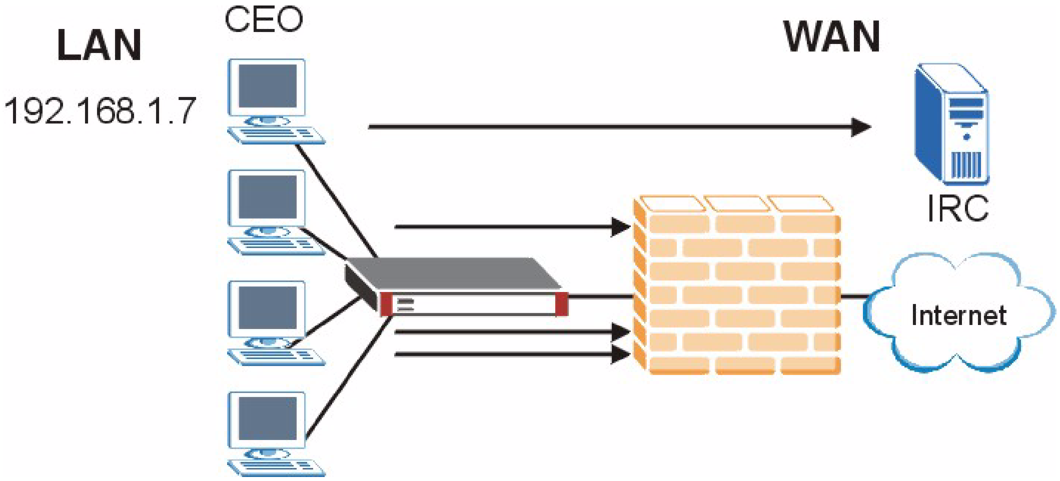
- Has a static IP address,

  or

- You configure a static DHCP entry for it so the ZyWALL always assigns it the same IP address (see Section 10.1.4 on page 182 for information on DHCP).

Now you configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

Figure 184 Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 86 Limited LAN to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
Default	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

Alternatively, you configure a LAN to WAN rule with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your firewall would have the following configuration.

Table 87 Limited LAN to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
Default	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN computer to access the IRC service on the WAN by logging into the ZyWALL with the CEO's user name.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

19.4 Alerts

You can choose to generate an alert or log when a rule is matched and have the ZyWALL send an immediate e-mail message to you. Otherwise, see the logs created (for the categories you specified) in the **View Log** screen. Refer to the chapter on logs for details.

19.5 Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.

You can have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate subnets.

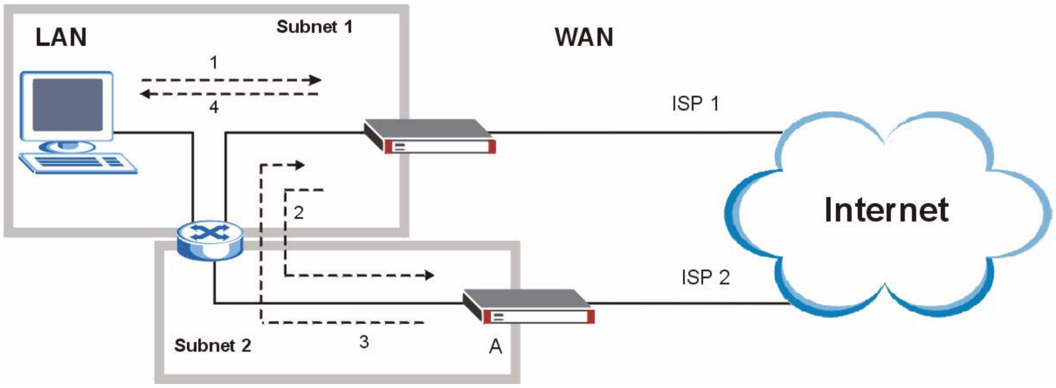
19.5.1 Virtual Interfaces and Asymmetrical Routes

You can use virtual interfaces instead of allowing asymmetrical routes. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyWALL to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyWALL reroutes the packet to Gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the ZyWALL.
4. The ZyWALL then sends it to the computer on the LAN in **Subnet 1**.

Figure 185 Triangle Route: Using Virtual Interfaces



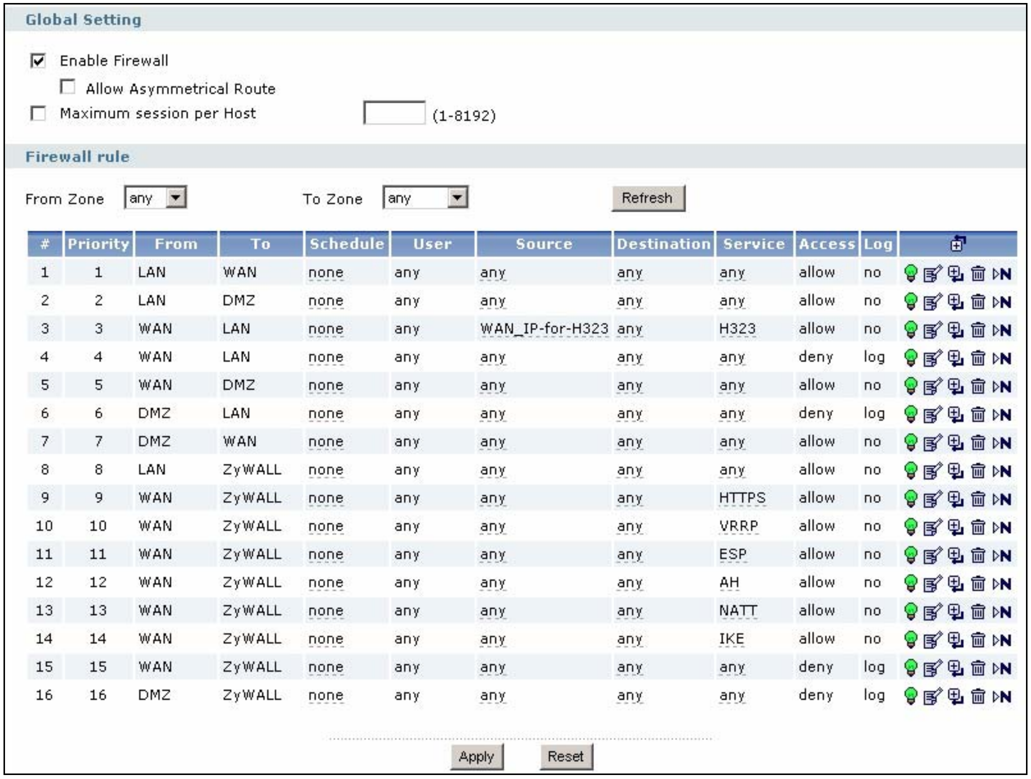
19.6 Configuring the Firewall

Click **Firewall** to open the **Firewall** screen. This screen varies depending on the firewall rule type and the way you choose to display the firewall rules.

The ordering of your rules is very important as rules are applied in sequence.

Specify from which zone packets come and to which zone packets travel to display only the rules specific to the selected direction.

Figure 186 Firewall



Global Setting

☑ Enable Firewall

☐ Allow Asymmetrical Route

☐ Maximum session per Host (1-8192)

Firewall rule

From Zone any To Zone any

#	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1	1	LAN	WAN	none	any	any	any	any	allow	no
2	2	LAN	DMZ	none	any	any	any	any	allow	no
3	3	WAN	LAN	none	any	WAN_IP-for-H323	any	H323	allow	no
4	4	WAN	LAN	none	any	any	any	any	deny	log
5	5	WAN	DMZ	none	any	any	any	any	allow	no
6	6	DMZ	LAN	none	any	any	any	any	deny	log
7	7	DMZ	WAN	none	any	any	any	any	allow	no
8	8	LAN	ZyWALL	none	any	any	any	any	allow	no
9	9	WAN	ZyWALL	none	any	any	any	HTTPS	allow	no
10	10	WAN	ZyWALL	none	any	any	any	VRRP	allow	no
11	11	WAN	ZyWALL	none	any	any	any	ESP	allow	no
12	12	WAN	ZyWALL	none	any	any	any	AH	allow	no
13	13	WAN	ZyWALL	none	any	any	any	NATT	allow	no
14	14	WAN	ZyWALL	none	any	any	any	IKE	allow	no
15	15	WAN	ZyWALL	none	any	any	any	any	deny	log
16	16	DMZ	ZyWALL	none	any	any	any	any	deny	log

The following table describes the labels in this screen.

Table 88 Firewall

LABEL	DESCRIPTION
Global Setting	
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control when the firewall is activated.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged. Select this check box to have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. See Section 19.5 on page 282 for an example.

Table 88 Firewall (continued)

LABEL	DESCRIPTION
Maximum session per host	Use this field to set the highest number of sessions that the ZyWALL will permit a computer with the same IP address to have at one time. When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyWALL. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using too many of the available NAT sessions.
From Zone To Zone	This is the direction of travel of packets. Select from which zone the packets come and to which zone the packets go. Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, from **LAN** to **LAN** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From **any** displays all the firewall rules for traffic going to a particular zone. To **any** displays all the firewall rules for traffic coming from a particular zone. From **any** to **any** displays all of the firewall rules. To **ZyWALL** rules are for traffic that is destined for the ZyWALL and control which computers can manage the ZyWALL.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction.	
#	This is the index number of your firewall rule. It is not associated with a specific rule.
Priority	This is the position of your firewall rule in the global rule list (including all through-ZyWALL and to-ZyWALL rules). The ordering of your rules is important as rules are applied in sequence.
Schedule	This field tells you the schedule object that the rule uses. **none** means the rule is active at all times if enabled.
User	This is the user name or user group name to which this firewall rule applies.
Source	This displays the source address object to which this firewall rule applies.
Destination	This displays the destination address object to which this firewall rule applies.
Service	This displays the service object to which this firewall rule applies.
Access	This field displays whether the firewall silently discards packets (**deny**), discards packets and sends a TCP reset packet to the sender (**reject**) or permits the passage of packets (**allow**).
Log	This field shows you whether a log (and alert) is created when packets match this rule or not.

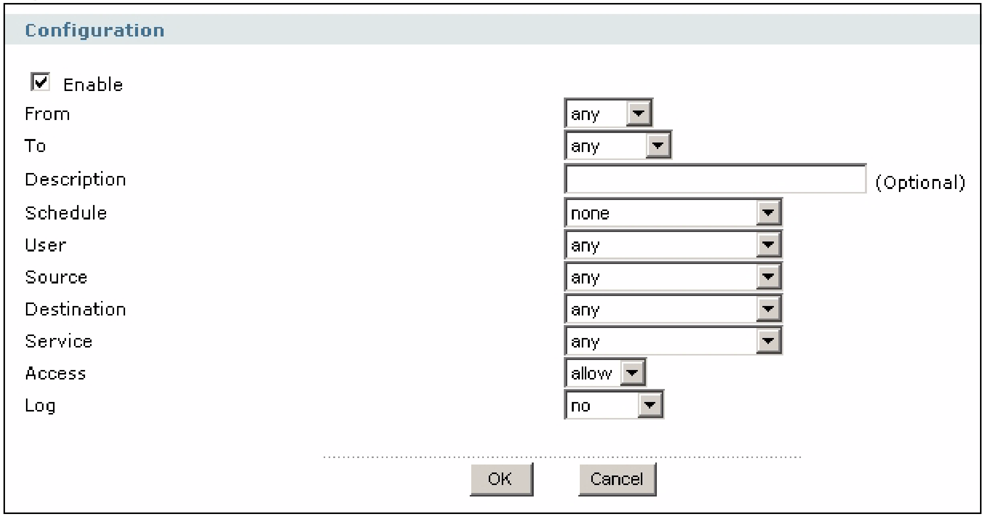
Table 88 Firewall (continued)

LABEL	DESCRIPTION
Add icon	Click the **Add** icon in the heading row to add a new first entry. The **Active** icon displays whether the rule is enabled or not. Click it to activate or deactivate the rule. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the rule on the ZyWALL. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. Note that subsequent firewall rules move up by one when you take this action. In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. For example, if you type 6, the rule you are moving becomes number 6 and the previous rule 6 (if there is one) gets pushed up (or down) one. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

19.6.1 Edit a Firewall Rule

In the **Firewall** screen, click the **Edit** or **Add** icon to display the **Firewall Rule Edit** screen. Refer to the following table for information on the labels.

Figure 187 Firewall > Edit



☑ Enable

From	any
To	any
Description	(Optional)
Schedule	none
User	any
Source	any
Destination	any
Service	any
Access	allow
Log	no

The following table describes the labels in this screen.

Table 89 Firewall > Edit

LABEL	DESCRIPTION
Enable	Select this check box to activate the firewall rule.
From To	For through-ZyWALL rules, select the direction of travel of packets to which the rule applies. **any** means all interfaces or VPN tunnels. **ZyWALL** means packets destined for the ZyWALL itself.

Table 89 Firewall > Edit (continued)

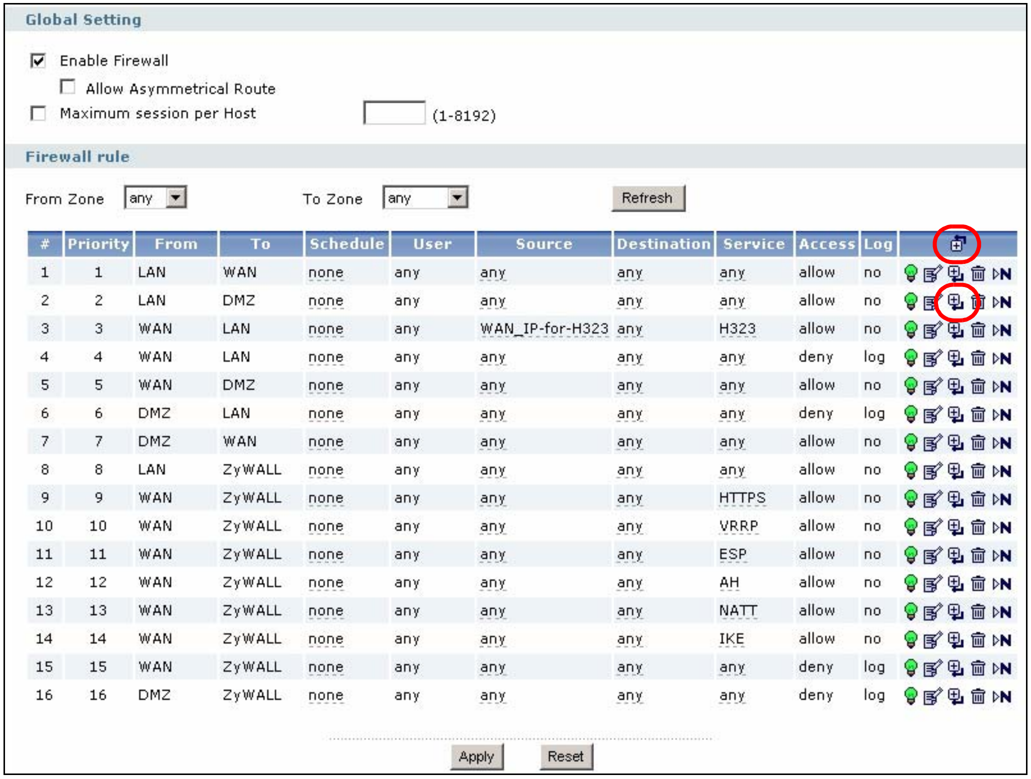
LABEL	DESCRIPTION
Description	Enter a descriptive name of up to 60 printable ASCII characters for the firewall rule. Spaces are allowed.
Schedule	Select a schedule that defines when the rule applies or select **Create Object** to configure a new one (see Chapter 37 on page 527 for details). Otherwise, select **none** and the rule is always effective.
User	This field is not available when you are configuring a to-ZyWALL rule. Select a user name or user group to which to apply the rule. Select **Create Object** to configure a new user account (see Section 34.2.1 on page 506 for details). The firewall rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified a source IP address (group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Source	Select a source address or address group for whom this rule applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group for whom this rule applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every destination.
Service	Select a service or service group from the drop-down list box. Select **Create Object** to add a new service. See Chapter 36 on page 521 for more information.
Access	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select **deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **reject** to deny the packets and send a TCP reset packet to the sender. Any UDP packets are dropped without sending a response packet. Select **allow** to permit the passage of the packets.
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or not (**no**) when the rule is matched.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

19.7 Firewall Rule Configuration Example

The following Internet firewall rule example allows a hypothetical MyService from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 (Dest_1) on the LAN.

1. Click **Firewall**. Click the **Add** icon (⊞) in the heading row to configure a new first entry (as in this example) or the **Add** icon (⊞) in an entry to add a rule below the selected entry. Remember the sequence (priority) of the rules is important since they are applied in order.

Figure 188 Firewall Example: Select the Traveling Direction of Traffic



Global Setting

☑ Enable Firewall
☐ Allow Asymmetrical Route
☐ Maximum session per Host (1-8192)

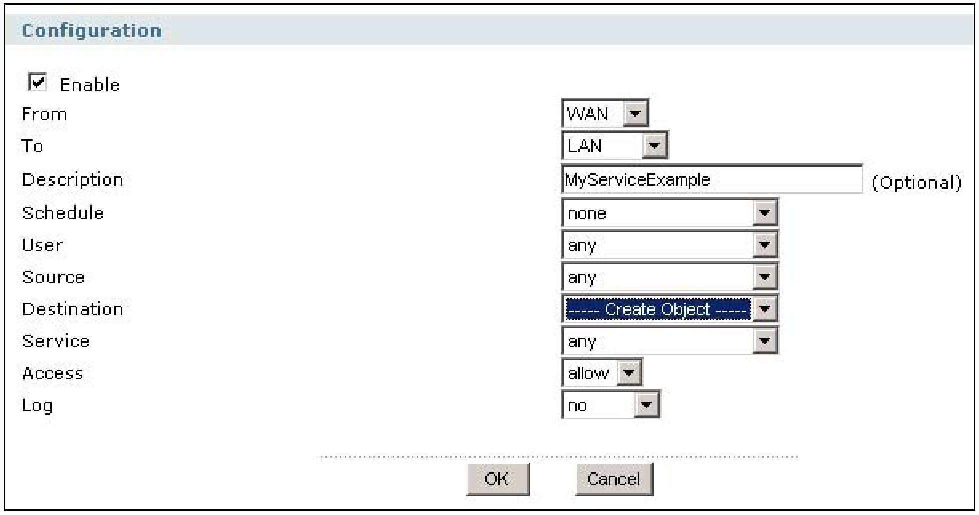
Firewall rule

From Zone: any   To Zone: any   Refresh

#	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1	1	LAN	WAN	none	any	any	any	any	allow	no
2	2	LAN	DMZ	none	any	any	any	any	allow	no
3	3	WAN	LAN	none	any	WAN_IP-for-H323	any	H323	allow	no
4	4	WAN	LAN	none	any	any	any	any	deny	log
5	5	WAN	DMZ	none	any	any	any	any	allow	no
6	6	DMZ	LAN	none	any	any	any	any	deny	log
7	7	DMZ	WAN	none	any	any	any	any	allow	no
8	8	LAN	ZyWALL	none	any	any	any	any	allow	no
9	9	WAN	ZyWALL	none	any	any	any	HTTPS	allow	no
10	10	WAN	ZyWALL	none	any	any	any	VRRP	allow	no
11	11	WAN	ZyWALL	none	any	any	any	ESP	allow	no
12	12	WAN	ZyWALL	none	any	any	any	AH	allow	no
13	13	WAN	ZyWALL	none	any	any	any	NATT	allow	no
14	14	WAN	ZyWALL	none	any	any	any	IKE	allow	no
15	15	WAN	ZyWALL	none	any	any	any	any	deny	log
16	16	DMZ	ZyWALL	none	any	any	any	any	deny	log

2 Select **From WAN** and **To LAN** and enter a description. Select **Create Object** in the **Destination** drop-down list box.

Figure 189 Firewall Example: Edit a Firewall Rule 1



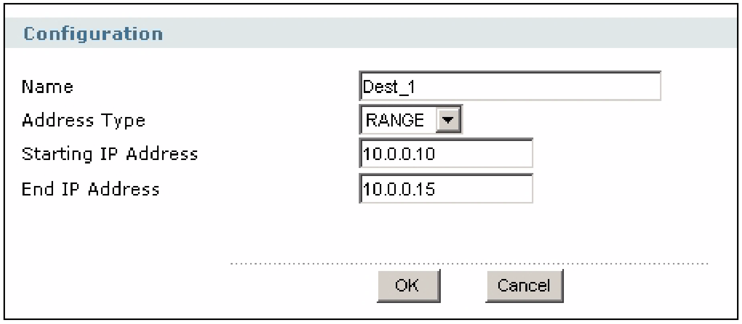
Configuration

☑ Enable

From	WAN
To	LAN
Description	MyServiceExample (Optional)
Schedule	none
User	any
Source	any
Destination	----- Create Object -----
Service	any
Access	allow
Log	no

3 The screen for configuring an address object opens. Configure it as follows and click **OK**.

Figure 190 Firewall Example: Create an Address Object

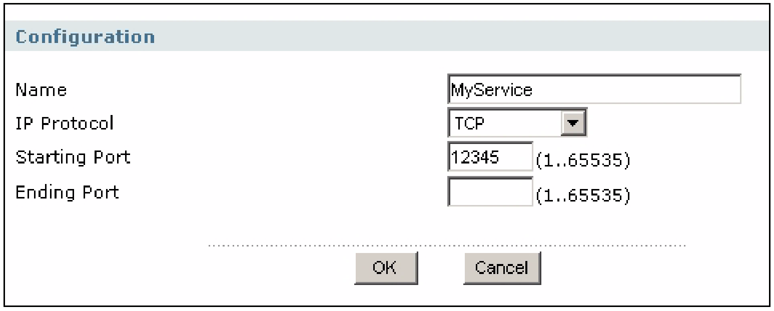


Name: Dest_1
Address Type: RANGE
Starting IP Address: 10.0.0.10
End IP Address: 10.0.0.15

4 Select **Create Object** in the **Service** drop-down list box.

5 The screen for configuring a service object opens. Configure it as follows and click **OK**.

Figure 191 Firewall Example: Create a Service Object

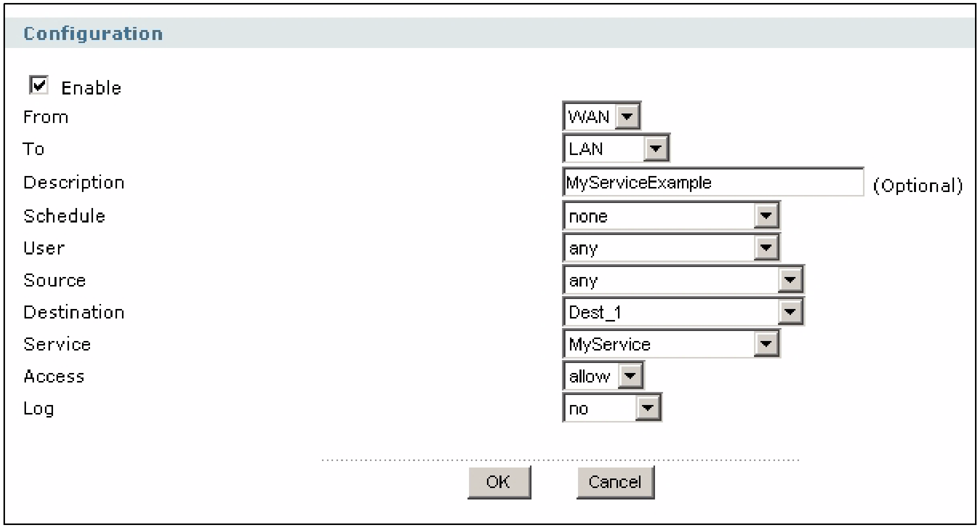


Name: MyService
IP Protocol: TCP
Starting Port: 12345 (1..65535)
Ending Port: (1..65535)

6 Enter the name of the firewall rule.

7 Make sure **Dest_1** is selected for the **Destination** and **MyService** is selected as the **Service** and that the rest of the screen is configured as follows. Click **OK** when you are done.

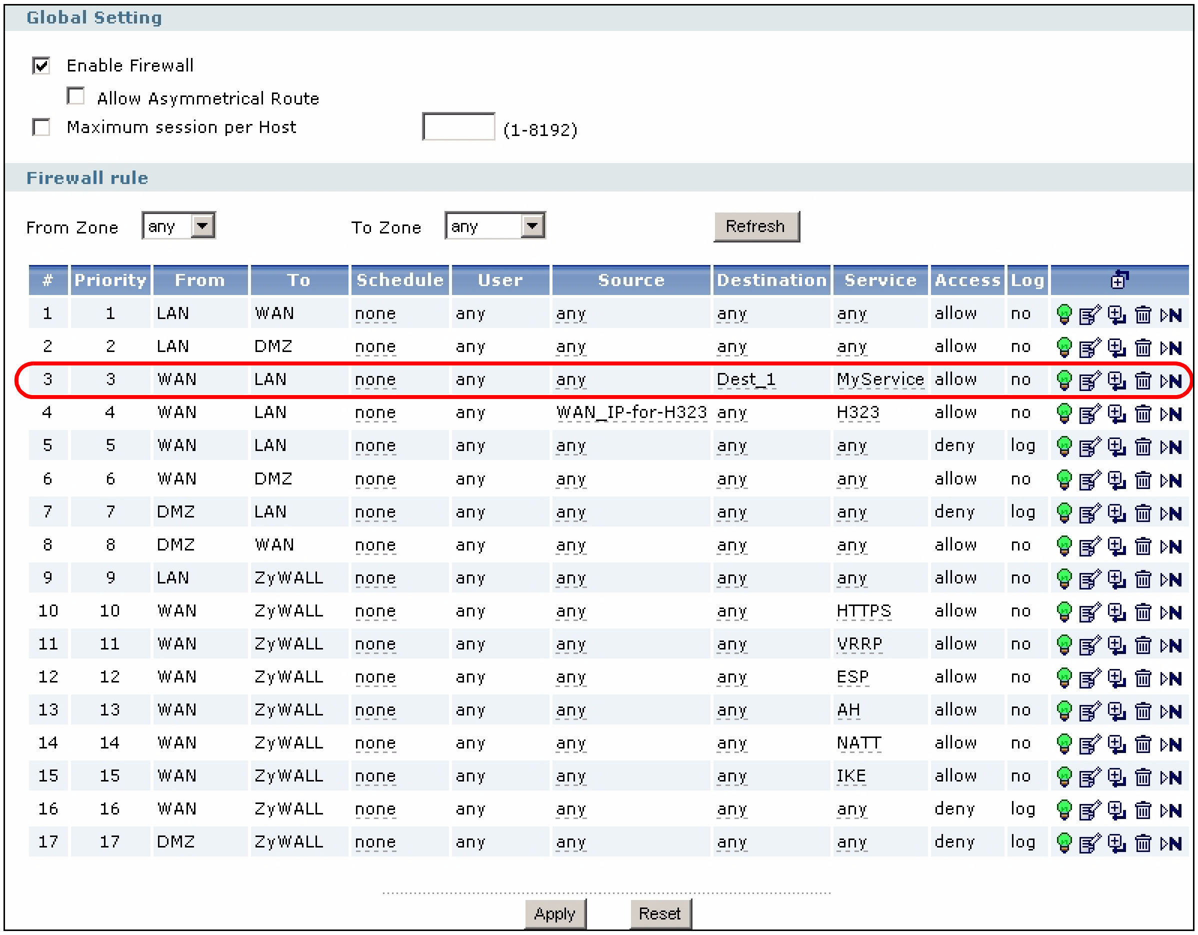
Figure 192 Firewall Example: Edit a Firewall Rule



☑ Enable
From: WAN
To: LAN
Description: MyServiceExample (Optional)
Schedule: none
User: any
Source: any
Destination: Dest_1
Service: MyService
Access: allow
Log: no

8 The firewall rule appears in the firewall rule summary.

Figure 193 Firewall Example: MyService Example Rule in Summary



☑ Enable Firewall

☐ Allow Asymmetrical Route

☐ Maximum session per Host (1-8192)

From Zone any

To Zone any

#	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1	1	LAN	WAN	none	any	any	any	any	allow	no
2	2	LAN	DMZ	none	any	any	any	any	allow	no
3	3	WAN	LAN	none	any	any	Dest_1	MyService	allow	no
4	4	WAN	LAN	none	any	WAN_IP-for-H323	any	H323	allow	no
5	5	WAN	LAN	none	any	any	any	any	deny	log
6	6	WAN	DMZ	none	any	any	any	any	allow	no
7	7	DMZ	LAN	none	any	any	any	any	deny	log
8	8	DMZ	WAN	none	any	any	any	any	allow	no
9	9	LAN	ZyWALL	none	any	any	any	any	allow	no
10	10	WAN	ZyWALL	none	any	any	any	HTTPS	allow	no
11	11	WAN	ZyWALL	none	any	any	any	VRRP	allow	no
12	12	WAN	ZyWALL	none	any	any	any	ESP	allow	no
13	13	WAN	ZyWALL	none	any	any	any	AH	allow	no
14	14	WAN	ZyWALL	none	any	any	any	NATT	allow	no
15	15	WAN	ZyWALL	none	any	any	any	IKE	allow	no
16	16	WAN	ZyWALL	none	any	any	any	any	deny	log
17	17	DMZ	ZyWALL	none	any	any	any	any	deny	log

20

IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyWALL. See Section 5.4.4 on page 116 for related information on these screens.

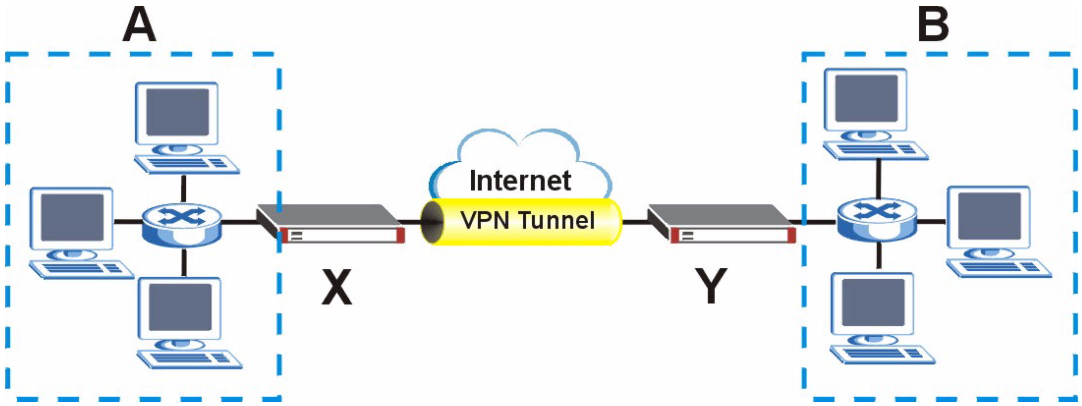
20.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure is one example of a VPN tunnel.

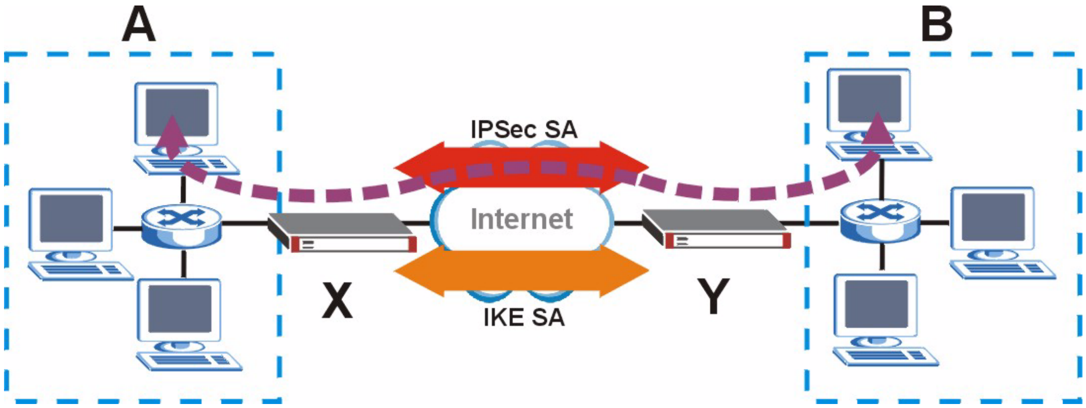
Figure 194 VPN: Example



The VPN tunnel connects the ZyWALL (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 195 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

The rest of this section discusses IKE SA and IPSec SA in more detail.

20.1.1 IPSec SA Overview

Once the ZyWALL and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

20.1.1.1 Local Network and Remote Network

In IPSec SA, the local network, the one(s) connected to the ZyWALL, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

20.1.1.2 Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

The ZyWALL and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

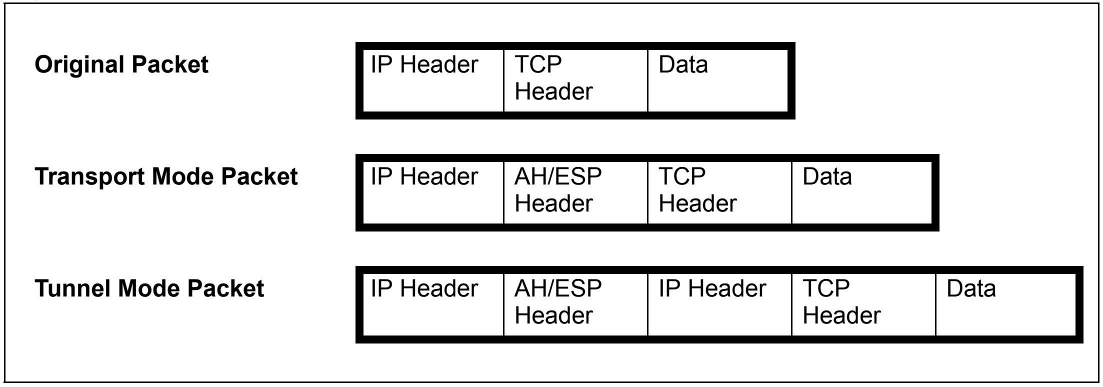
20.1.1.3 Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the ZyWALL and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

The ZyWALL and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 196 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the ZyWALL uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ZyWALL or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ZyWALL or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ZyWALL includes part of the original IP header when it encapsulates the packet. With ESP, however, the ZyWALL does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

20.1.1.4 IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see Section 20.4.1.2 on page 307), except that you also have the choice whether or not the ZyWALL and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyWALL and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the ZyWALL and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

20.1.2 Additional Topics for IPSec SA

This section provides more information about IPSec SA in your ZyWALL.

20.1.2.1 IPSec SA using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the ZyWALL and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

20.1.2.1.1 IPSec SA Proposal using Manual Keys

In IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ZyWALL and remote IPSec router use.

The ZyWALL and remote IPSec router must use the same encryption key and authentication key.

20.1.2.1.2 Authentication and the Security Parameter Index (SPI)

For authentication, the ZyWALL and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

The ZyWALL and remote IPSec router must use the same SPI.

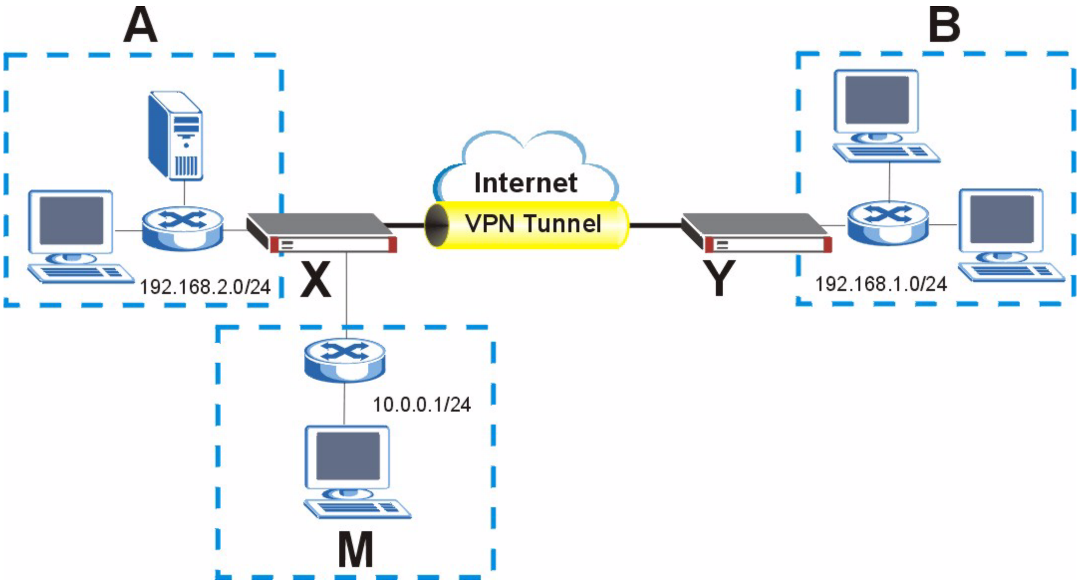
20.1.2.2 NAT for Inbound and Outbound Traffic

The ZyWALL can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 197 VPN Example: NAT for Inbound and Outbound Traffic



20.1.2.2.1 Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the ZyWALL route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 197 on page 295, you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPSec router may not route messages for computer **M** through the IPSec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.
- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

20.1.2.2.2 Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).

- Destination - the original destination address; the local network (**A**).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

20.1.2.2.3 Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the ZyWALL to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 197 on page 295, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The ZyWALL checks these rules similar to the way it checks rules for a firewall. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 197 on page 295, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

- Mapped IP - the translated destination address; in Figure 197 on page 295, the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

20.2 VPN Related Configuration

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the ZyWALL uses IP address when it establishes the IKE SA. You should set up the interface first. See Chapter 10 on page 179.
- In a VPN gateway, you can enable extended authentication. If the ZyWALL runs in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the ZyWALL authenticates the remote IPSec router. See Chapter 38 on page 531.
- In a VPN gateway, the ZyWALL and remote IPSec router can use certificates to authenticate each other. You should import the certificate first. See Chapter 40 on page 545.

You should set up the following features before the network can use the VPN tunnel.

- The ZyWALL does not put IPSec SA in the routing table. You must create a policy route for the VPN tunnel. See Chapter 12 on page 225.

- Make sure the to-ZyWALL firewall rules allow IPSec VPN traffic to the ZyWALL. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The ZyWALL supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the to-ZyWALL firewall rules allow UDP port 4500 too.
- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the ZyWALL sends before the ZyWALL encrypts them and check packets the ZyWALL receives after the ZyWALL decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP.

If there are problems setting up a VPN tunnel, make sure both the ZyWALL and remote IPSec router have the same settings for the VPN tunnel. It is also helpful to have a way to look at the packets that are being sent and received by the ZyWALL and remote IPSec router (for example, packet sniffers).

20.3 VPN Connection Screens

You use the **VPN Connection** summary screen to look at the VPN connections you have set up, and you use the **VPN Connection Add/Edit Manual Key** and **VPN Connection Add/ Edit Gateway** screens to create or to edit VPN connections.

20.3.1 VPN Connection Summary

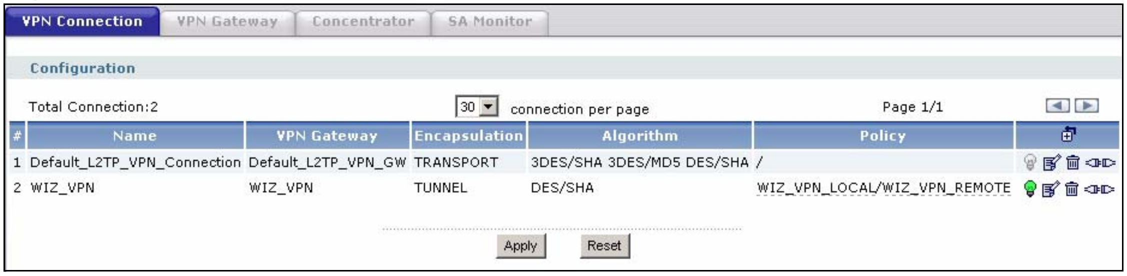
The **VPN Connection** summary screen displays the list of VPN connections, the associated VPN gateway(s), and various settings. In addition, it also lets you activate / deactivate and connect / disconnect each VPN connection (each IPSec SA).

To access this screen, click **VPN** > **IPSec VPN**. The following screen appears.

Each VPN connection requires a corresponding policy route.

The VPN wizard automatically creates a corresponding policy route. If you create the VPN connection in the **VPN > IPSec VPN** screens, you need to manually create a corresponding policy route.

Figure 198 VPN > IPSec VPN > VPN Connection



Total Connection:2

30 connection per page

Page 1/1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TRANSPORT	3DES/SHA 3DES/MD5 DES/SHA	/	
2	WIZ_VPN	WIZ_VPN	TUNNEL	DES/SHA	WIZ_VPN_LOCAL/WIZ_VPN_REMOTE	

Each field is discussed in the following table. See Section 20.3.3 on page 302 and Section 20.3.2 on page 298 for more information.

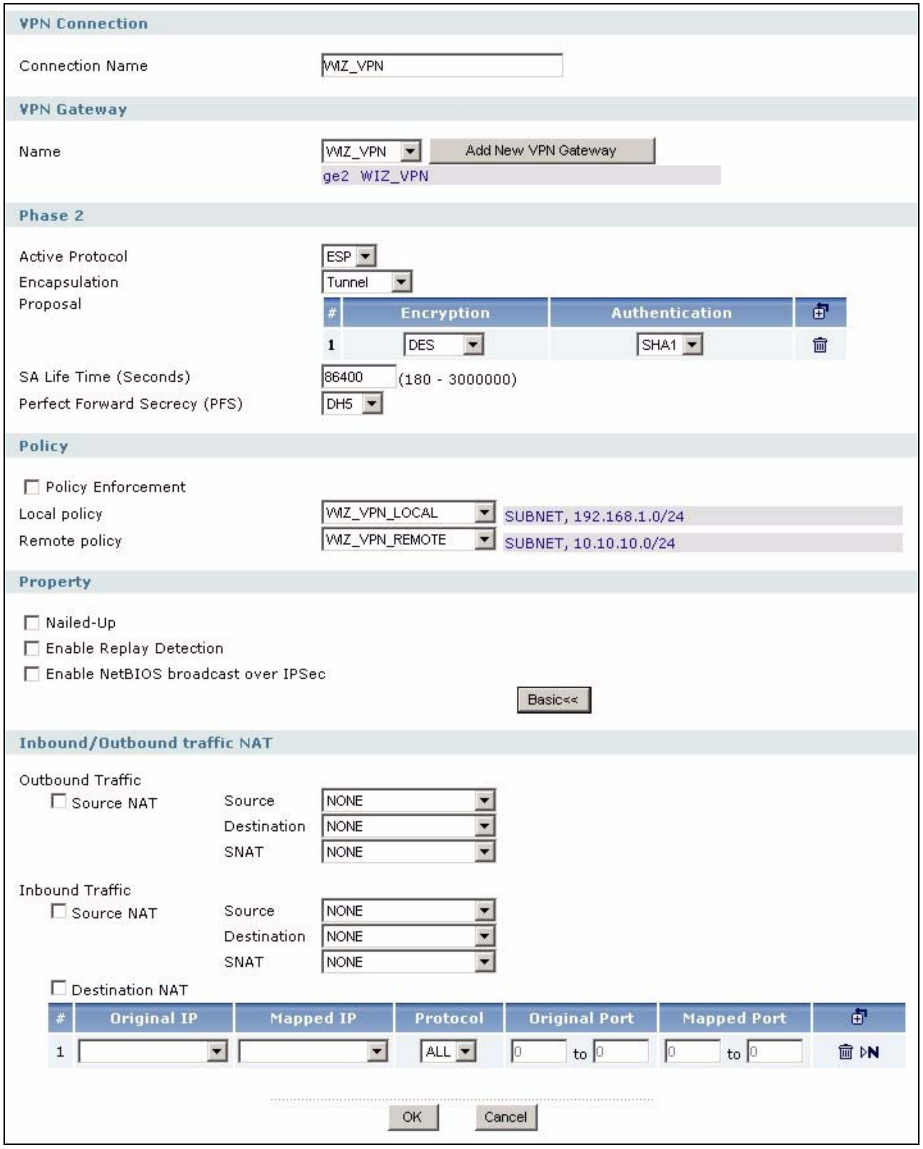
Table 90 VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific connection.
Name	This field displays the name of the IPSec SA.
VPN Gateway	This field displays the associated VPN gateway(s). If there is no VPN gateway, this field displays “manual key”.
Encapsulation	This field displays what encapsulation the IPSec SA uses.
Algorithm	This field displays what encryption and authentication methods, respectively, the IPSec SA uses.
Policy	This field displays the local policy and the remote policy, respectively.
Add icon	This column provides icons to add, edit, and remove VPN connections, as well as to activate / deactivate and connect / disconnect VPN connections. To add a VPN connection, click the **Add** icon at the top of the column. The **VPN Connection Add/Edit Manual** screen appears. To edit a VPN connection, click the **Edit** icon next to the connection. The **VPN Connection Add/Edit Manual** or **VPN Connection Add/Edit Gateway** screen appears accordingly. To delete a VPN connection, click the **Remove** icon next to the connection. The web configurator confirms that you want to delete the VPN connection. To activate or deactivate an IPSec SA, click the **Active** icon next to the VPN connection. Make sure you click **Apply** to save and apply the change. To connect or disconnect an IPSec SA, click the **Connect** icon next to the VPN connection.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

20.3.2 VPN Connection Add/Edit IKE

The **VPN Connection Add/Edit Gateway** screen allows you to create a new VPN connection using a VPN gateway (with IKE) or edit an existing VPN connection using a VPN gateway. To access this screen, go to the **VPN Connection Summary** screen (see Section 20.3.1 on page 297), and click either the **Add** icon or an **Edit** icon. If you click the **Add** icon, you have to select a specific VPN gateway in the **VPN Gateway** field before the following screen appears.

Figure 199 VPN > IPSec VPN > VPN Connection > Edit (IKE)



VPN Connection

Connection Name: WIZ_VPN

VPN Gateway

Name: WIZ_VPN

ge2 WIZ_VPN

Phase 2

Active Protocol: ESP
Encapsulation: Tunnel
Proposal

#	Encryption	Authentication
1	DES	SHA1

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): DH5

Policy

☐ Policy Enforcement
Local policy: WIZ_VPN_LOCAL SUBNET, 192.168.1.0/24
Remote policy: WIZ_VPN_REMOTE SUBNET, 10.10.10.0/24

Property

☐ Nailed-Up
☐ Enable Replay Detection
☐ Enable NetBIOS broadcast over IPSec

Inbound/Outbound traffic NAT

Outbound Traffic
☐ Source NAT
Source: NONE
Destination: NONE
SNAT: NONE

Inbound Traffic
☐ Source NAT
Source: NONE
Destination: NONE
SNAT: NONE

☐ Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
1			ALL	0 to 0	0 to 0

Each field is described in the following table.

Table 91 VPN > IPSec VPN > VPN Connection > Edit

LABEL	DESCRIPTION
VPN Connection	
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
VPN Gateway	
Name	Select the VPN gateway that you want to use with this VPN connection.
Add New VPN Gateway	Click this button to add another VPN gateway this VPN connection can use.
Phase 2	

Table 91 VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication** algorithm. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption** algorithm and **Authentication** algorithm. Both **AH** and **ESP** increase processing requirements and latency (delay).
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data **Transport** - this mode only encrypts the data
Proposal	
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES128 - a 128-bit key with the AES encryption algorithm AES192 - a 192-bit key with the AES encryption algorithm AES256 - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same key. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Add icon	This column contains icons to add and remove proposals. To add a proposal, click the **Add** icon at the top of the column. To remove a proposal, click the **Remove** icon next to the proposal. The ZyWALL confirms that you want to delete it before doing so.
SA Life Time (Seconds)	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The ZyWALL automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **none** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number **DH5** - enable PFS and use a 1536-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. It is more secure but takes more time.
Policy	

Table 91 VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Policy Enforcement	Select this if you want the ZyWALL to drop traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPSec SA more secure. Note: You must clear this field, however, if you want to use the IPSec SA in a VPN concentrator.
Local Policy	Select the address or address group corresponding to the local network. Select **Create Object** to configure a new one.
Remote Policy	Select the address or address group corresponding to the remote network. Select **Create Object** to configure a new one.
Property	
Nailed-Up	Select this if you want the ZyWALL to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	Select this check box if you the ZyWALL to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
Advanced/Basic	Click this button to show or hide the **Inbound/Outbound traffic NAT** fields.
Inbound/Outbound traffic NAT	Click the **Advanced** or **Basic** button to show or hide this section.
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address object for the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the remote network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the local network.

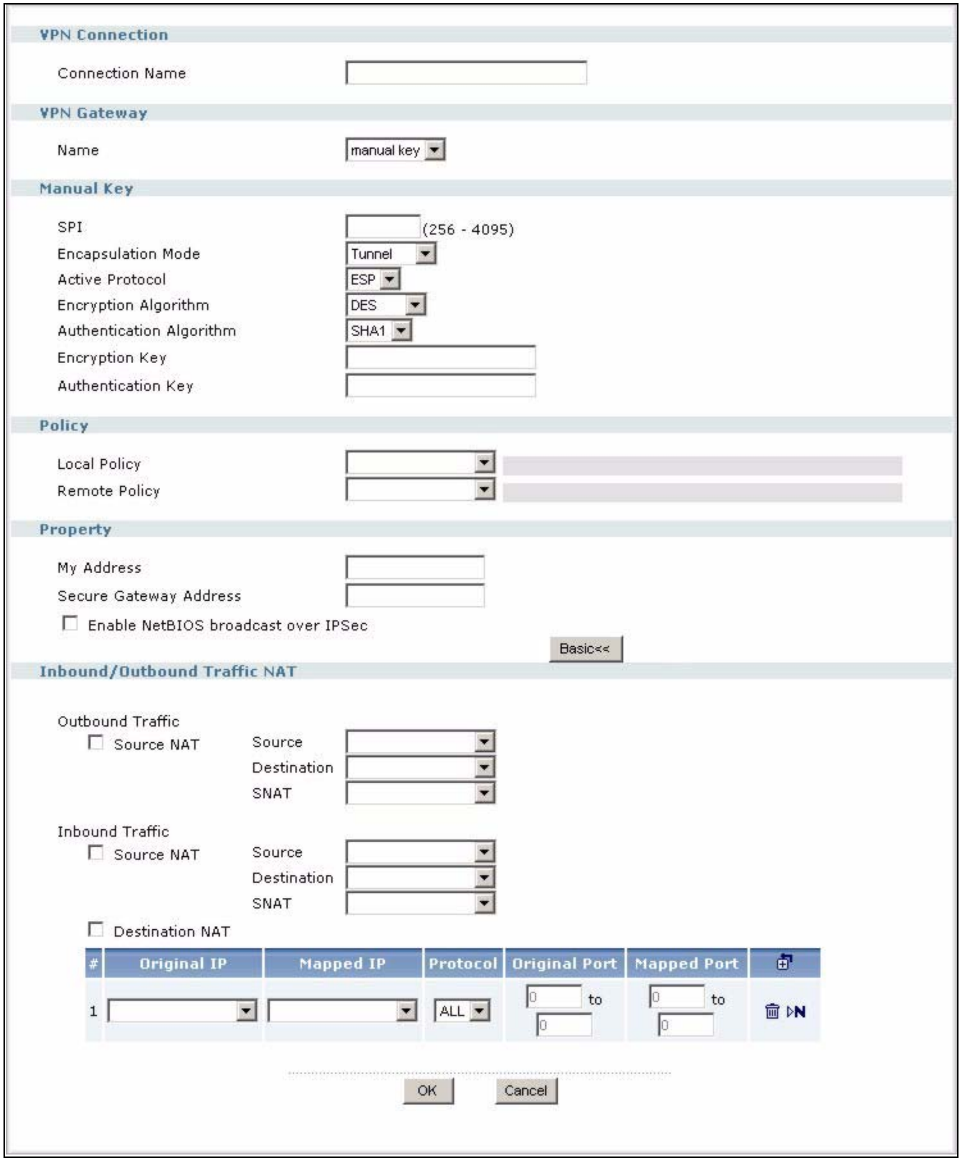
Table 91 VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address that hides the original source address. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, or **All**.
Original Port	These fields are available if the protocol is **TCP** or **UDP**. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port	These fields are available if the protocol is **TCP** or **UDP**. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Add icon	This column contains icons to add, move, and remove NAT records. To add a NAT record, click the **Add** icon at the top of the column. To move a NAT record, click the **Move to N** icon next to the record, and then type the row number to which you want to move it. The records are renumbered automatically. To remove a NAT record, click the **Remove** icon next to the record. The ZyWALL confirms that you want to delete the NAT record before doing so.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

20.3.3 VPN Connection Add/Edit Manual Key

The **VPN Connection Add/Edit Manual Key** screen allows you to create a new VPN connection or edit an existing one using a manual key. This is useful if you have problems with IKE key management. To access this screen, go to the **VPN Connection** summary screen (see Section 20.3.1 on page 297), and click either the **Add** icon or an existing manual key entry's **Edit** icon.

Figure 200 VPN > IPSec VPN > VPN Connection > Manual Key > Edit



Name: manual key

SPI (256 - 4095)

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

#	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
1			ALL	0 to 0	0 to 0

VPN Connection
Connection Name
VPN Gateway
Manual Key
Encryption Key
Authentication Key
Policy
Local Policy
Remote Policy
Property
My Address
Secure Gateway Address
☐ Enable NetBIOS broadcast over IPSec
Basic<<
Inbound/Outbound Traffic NAT
Outbound Traffic
☐ Source NAT
Source
Destination
SNAT
Inbound Traffic
☐ Source NAT
Source
Destination
SNAT
☐ Destination NAT
OK
Cancel

The following table describes the labels in this screen.

Table 92 VPN > IPSec VPN > VPN Connection > Manual Key > Edit

LABEL	DESCRIPTION
VPN Connection	
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
VPN Gateway	
Name	Select **manual key** in the drop-down list.
Manual Key	
SPI	Type a unique **SPI** (Security Parameter Index) between 256 and 4095. The SPI is used to identify the ZyWALL during authentication.

Table 92 VPN > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

LABEL	DESCRIPTION
Encapsulation Mode	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data **Transport** - this mode only encrypts the data. You should only select this if the IPSec SA is used for communication between the ZyWALL and remote IPSec router. If you select **Transport** mode, the ZyWALL automatically switches to **Tunnel** mode if the IPSec SA is not used for communication between the ZyWALL and remote IPSec router. In this case, the ZyWALL generates a log message for this change.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication Algorithm**. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption Algorithm** and **Authentication Algorithm**.
Encryption Algorithm	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Encryption Key	This field is applicable when you select an **Encryption Algorithm**. Enter the encryption key, which depends on the encryption algorithm. **DES** - type a unique key 8-32 characters long **3DES** - type a unique key 24-32 characters long **AES128** - type a unique key 16-32 characters long **AES192** - type a unique key 24-32 characters long **AES256** - type a unique key 32 characters long You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The remote IPSec router must have the same encryption key. The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter `1234567890XYZ` for a DES encryption key, the ZyWALL only uses `12345678`. The ZyWALL still stores the longer key.

Table 92 VPN > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

LABEL	DESCRIPTION
Authentication Key	Enter the authentication key, which depends on the authentication algorithm. **MD5** - type a unique key 16-20 characters long **SHA1** - type a unique key 20 characters long You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The remote IPSec router must have the same authentication key. The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter `12345678901234567890` for a MD5 authentication key, the ZyWALL only uses `1234567890123456`. The ZyWALL still stores the longer key.
Policy	You can set up overlapping local policies or overlapping remote policies in the ZyWALL.
Local Policy	Select the address or address group corresponding to the local network. Select **Create Object** to configure a new one.
Remote Policy	Select the address or address group corresponding to the remote network. Select **Create Object** to configure a new one.
Property	
My Address	Type the IP address of the ZyWALL in the IPSec SA. 0.0.0.0 is invalid.
Secure Gateway Address	Type the IP address of the remote IPSec router in the IPSec SA.
Enable NetBIOS broadcast over IPSec	Select this check box if you want the ZyWALL to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
Advanced/Basic	Click this button to show or hide the **Inbound/Outbound traffic NAT** fields.
Inbound/ Outbound traffic NAT	Click the **Advanced** or **Basic** button to show or hide this section.
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address object for the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Inbound Traffic	

Table 92 VPN > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

LABEL	DESCRIPTION
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the remote network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the local network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address that hides the original source address. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, or **All**.
Original Port	This field is available if the protocol is **TCP** or **UDP**. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port	This field is available if the protocol is **TCP** or **UDP**. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Add icon	This column contains icons to add, move, and remove NAT records. To add a NAT record, click the **Add** icon at the top of the column. To move a NAT record, click the **Move to N** icon next to the record, and then type the row number to which you want to move it. The records are renumbered automatically. To remove a NAT record, click the **Remove** icon next to the record. The ZyWALL confirms that you want to delete the NAT record before doing so.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

20.4 VPN Gateway Screens

You use the **VPN Gateway** summary screen to look at the VPN gateways you have set up, and you use the **VPN Gateway Add/Edit** screen to create or to edit VPN gateways.

20.4.1 IKE SA Overview

The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Both routers must use the same negotiation mode.

These modes are discussed in more detail in Section 20.4.2.1 on page 310. Main mode is used in various examples in the rest of this section.

20.4.1.1 IP Addresses of the ZyWALL and Remote IPSec router

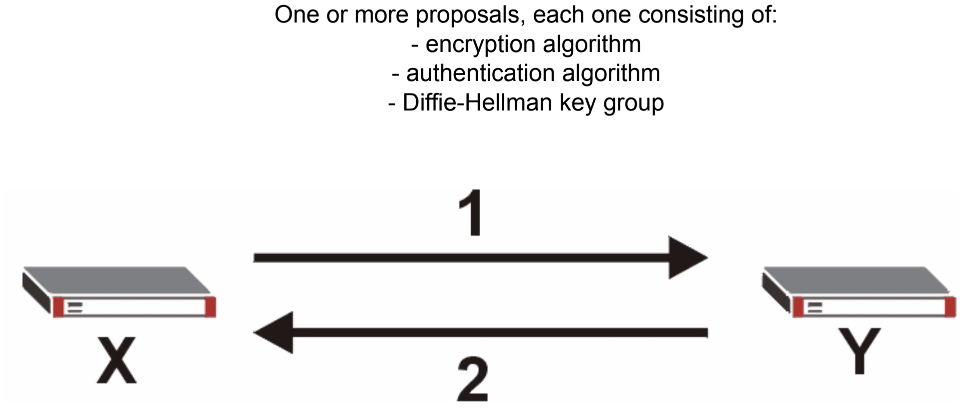
To set up an IKE SA, you have to specify the IP addresses of the ZyWALL and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your ZyWALL might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the ZyWALL does not know the IP address of the remote IPSec router. This is often used for telecommuters.

20.4.1.2 IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyWALL and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 201 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal


One or more proposals, each one consisting of:
- encryption algorithm
- authentication algorithm
- Diffie-Hellman key group
1
X
2
Y

The ZyWALL sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyWALL wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. If the remote IPSec router rejects all of the proposals, the ZyWALL and remote IPSec router cannot establish an IKE SA.

Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some ZyWALLs also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most ZyWALLs, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

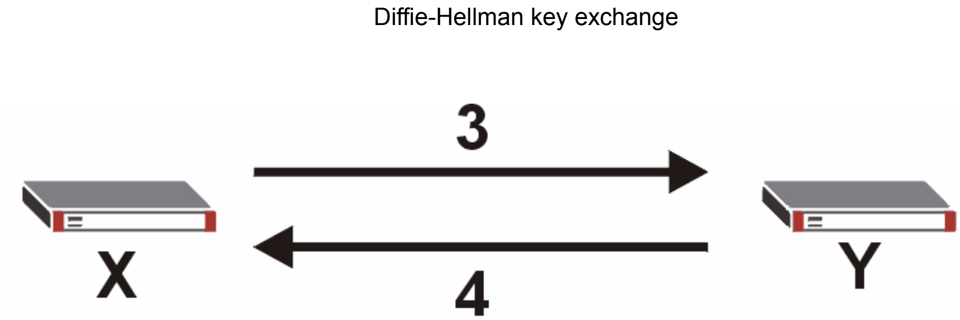
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

See Section 20.4.1.3 on page 308 for more information about DH key groups.

20.4.1.3 Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 202 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

20.4.1.4 Authentication

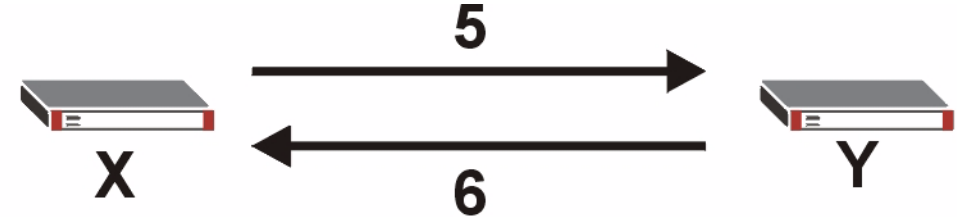
Before the ZyWALL and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyWALL and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

Figure 203 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)

Step 5:
pre-shared key
ZyWALL identity, consisting of
- ID type
- content

Step 6:
pre-shared key
Remote IPSec router identity, consisting of
- ID type
- content



You have to create (and distribute) a pre-shared key. The ZyWALL and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

The ZyWALL and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any domain name or e-mail address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the ZyWALL's or remote IPSec router's properties.

The ZyWALL and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

The ZyWALL's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in Table 93 on page 310, the ZyWALL and the remote IPSec router authenticate each other successfully. In contrast, in Table 94 on page 310, the ZyWALL and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 93 VPN Example: Matching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

Table 94 VPN Example: Mismatching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the ZyWALL to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your ZyWALL provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

20.4.2 Additional Topics for IKE SA

This section provides more information about IKE SA.

20.4.2.1 Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The ZyWALL sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL.

Steps 3 - 4: The ZyWALL and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

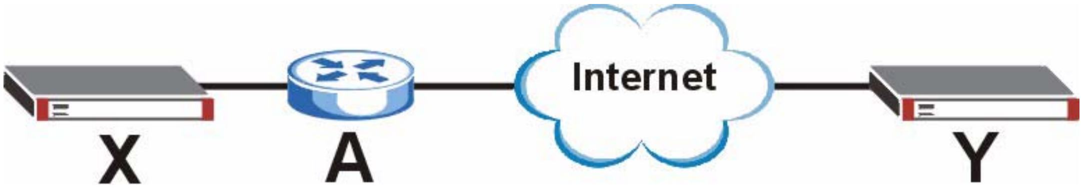
Steps 5 - 6: Finally, the ZyWALL and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

20.4.2.2 VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 204 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Section 20.1.1.2 on page 292 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyWALL and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyWALL and remote IPSec router support.

20.4.2.3 Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyWALL to provide a user name and password to the remote IPSec router, or you can set up the ZyWALL to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

20.4.2.4 Certificates

It is possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

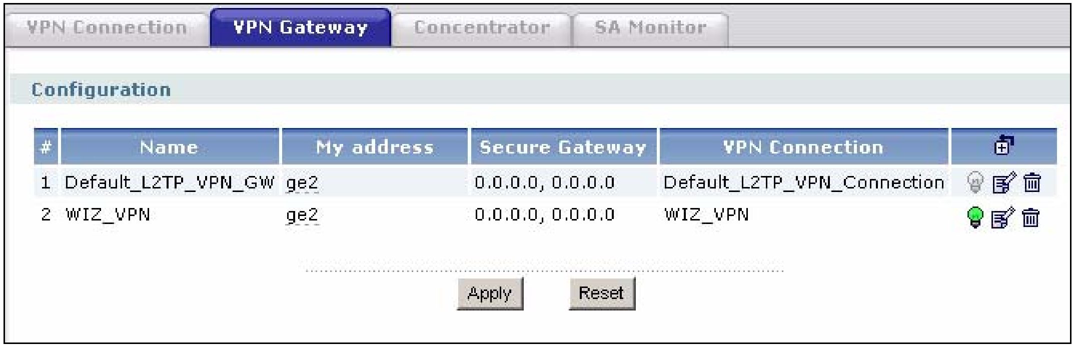
You must set up the certificates for the ZyWALL and remote IPSec router first.

20.4.3 VPN Gateway Summary

The **VPN Gateway** summary screen displays the VPN gateways in the ZyWALL, as well as the ZyWALL's address, remote IPSec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway.

To access this screen, click **VPN** > **Network** > **IPSec VPN** > **VPN Gateway**. The following screen appears.

Figure 205 VPN > IPSec VPN > VPN Gateway



#	Name	My address	Secure Gateway	VPN Connection
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection
2	WIZ_VPN	ge2	0.0.0.0, 0.0.0.0	WIZ_VPN

Each field is discussed in the following table. See Section 20.4.4 on page 313 for more information.

Table 95 VPN > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific gateway.
Name	This field displays the name of the VPN gateway.
My address	This field displays the address of the VPN gateway. The address can be an interface or a domain name.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.

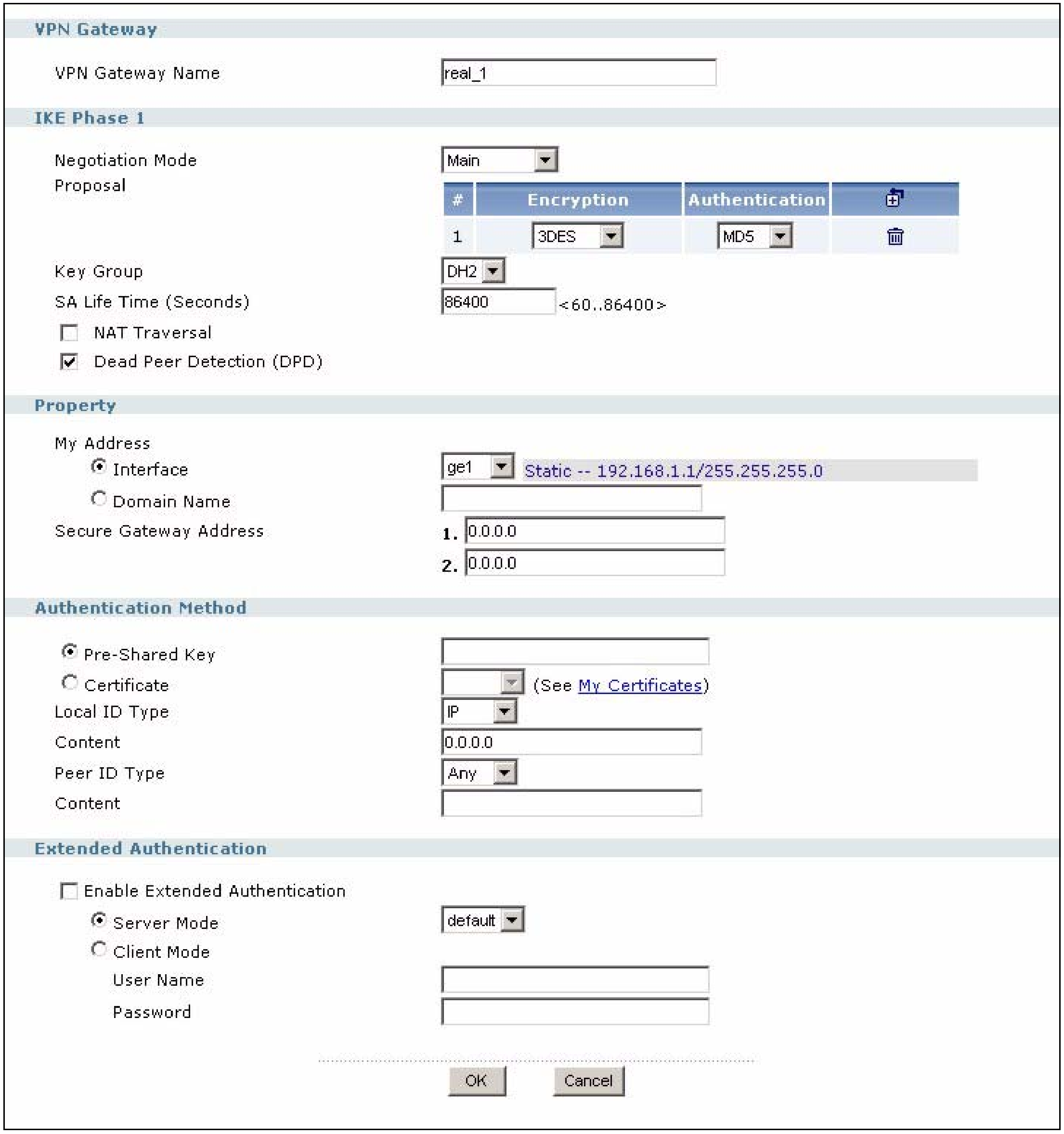
Table 95 VPN > IPSec VPN > VPN Gateway (continued)

LABEL	DESCRIPTION
Add icon	This column provides icons to add, edit, and remove VPN gateways, as well as to activate / deactivate VPN gateways. To add a VPN gateway, click the **Add** icon at the top of the column. The **VPN Gateway Add/Edit** screen appears. To edit a VPN gateway, click the **Edit** icon next to the gateway. The **VPN Gateway Add/Edit** screen appears accordingly. To delete a VPN gateway, click on the **Remove** icon next to the gateway. The web configurator confirms that you want to delete the VPN gateway. To activate or deactivate a VPN gateway, click the **Active** icon next to the gateway. Make sure you click **Apply** to save and apply the change.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

20.4.4 VPN Gateway Add/Edit

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway or edit an existing one. To access this screen, go to the **VPN Gateway** summary screen (see Section 20.4.3 on page 312), and click either the **Add** icon or an **Edit** icon.

Figure 206 VPN > IPSec VPN > VPN Gateway > Edit



VPN Gateway Name: real_1

Negotiation Mode: Main

Proposal:

#	Encryption	Authentication
1	3DES	MD5

Key Group: DH2

SA Life Time (Seconds): 86400 <60..86400>

☐ NAT Traversal

☑ Dead Peer Detection (DPD)

My Address

● Interface: ge1 Static -- 192.168.1.1/255.255.255.0

○ Domain Name

Secure Gateway Address: 1. 0.0.0.0 2. 0.0.0.0

● Pre-Shared Key

○ Certificate (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content:

☐ Enable Extended Authentication

● Server Mode: default

○ Client Mode

User Name:

Password:

Each field is described in the following table.

Table 96 VPN > IPSec VPN > VPN Gateway > Edit

LABEL	DESCRIPTION
VPN Gateway	
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IKE Phase 1	
Negotiation Mode	Select which negotiation mode you want to use to negotiate the IKE SA. Choices are **Main** - this encrypts the ZyWALL's and remote IPSec router's identities but takes more time to establish the IKE SA **Aggressive** - this is faster but does not encrypt the identities The ZyWALL and the remote IPSec router must use the same negotiation mode.

Table 96 VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Proposal	
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same key. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Add icon	This column contains icons to add and remove protocols. To add a protocol, click the **Add** icon at the top of the column. To remove a protocol, click the **Remove** icon next to the protocol. The ZyWALL confirms that you want to delete the protocol before doing so.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the ZyWALL and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SA that use active protocol AH. • There are one or more NAT routers between the ZyWALL and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.
Dead Peer Detection (DPD)	Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec server. If the remote IPSec server responds, the ZyWALL transmits the data. If the remote IPSec server does not respond, the ZyWALL shuts down the IKE SA.
Property	
My Address	Select how the IP address of the ZyWALL in the IKE SA is defined. Choices are **Interface** and **Domain Name**. If you select **Interface**, you must select an Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface, PPPoE/PPTP interface, or auxiliary interface. The IP address of the ZyWALL in the IKE SA is the IP address of the interface. If you select **Domain Name**, you must provide the domain name or the IP address of the ZyWALL. The IP address of the ZyWALL in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is invalid. If you change this value, the ZyWALL has to re-build the IKE SA.

Table 96 VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Secure Gateway Address	Type the IP address or the domain name of the remote IPSec router. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic IP address. You can provide a second IP address or domain name. In this case, if the ZyWALL cannot establish an IKE SA with the first one, it tries to establish an IKE SA with the second one.
Authentication Method	Note: The ZyWALL and remote IPSec router must use the same authentication method to establish the IKE SA.
Pre-Shared Key	Select this if the ZyWALL and remote IPSec router do not use certificates to identify each other when they negotiate the IKE SA. Then, type the pre-shared key in the field to the right. The pre-shared key can be • 8 - 32 alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • 16 - 64 hexadecimal (0-9, A-F) characters, preceded by “0x”. If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The ZyWALL and remote IPSec router must use the same pre-shared key.
Certificate	Select this if the ZyWALL and remote IPSec router use certificates to identify each other when they negotiate the IKE SA. Then, select the certificate the remote IPSec router uses to identify the ZyWALL. This certificate is one of the certificates in **My Certificates**. Note: The ZyWALL must import the remote IPSec router’s certificate before it can establish the IKE SA. The ZyWALL uses one of its **Trusted Certificates** to authenticate the remote IPSec router. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router’s certificate.
Local ID Type	This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the ZyWALL during authentication. Choices are: **IP** - the ZyWALL is identified by an IP address **DNS** - the ZyWALL is identified by a domain name **E-mail** - the ZyWALL is identified by an e-mail address
Content	This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Type the identity of the ZyWALL during authentication. The identity depends on the **Local ID Type**. **IP** - type an IP address; if you type 0.0.0.0, the ZyWALL uses the IP address specified in the **My Address** field. This is not recommended in the following situations: • There is a NAT router between the ZyWALL and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Local ID Type**. **DNS** - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. **E-mail** - the ZyWALL is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.

Table 96 VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Peer ID Type	Select which type of identification is used to identify the remote IPSec router during authentication. Choices are: **IP** - the remote IPSec router is identified by an IP address **DNS** - the remote IPSec router is identified by a domain name **E-mail** - the remote IPSec router is identified by an e-mail address **Any** - the ZyWALL does not check the identity of the remote IPSec router If the ZyWALL and remote IPSec router use certificates, there is one more choice. **Subject Name** - the remote IPSec router is identified by the subject name in the certificate
Content	This field is disabled if the **Peer ID Type** is **Any**. Type the identity of the remote IPSec router during authentication. The identity depends on the **Peer ID Type**. If the ZyWALL and remote IPSec router do not use certificates, **IP** - type an IP address; see the note at the end of this description. **DNS** - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. **E-mail** - the ZyWALL is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. If the ZyWALL and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router. **IP** - subject alternative name field; see the note at the end of this description. **DNS** - subject alternative name field **E-mail** - subject alternative name field **Subject Name** - subject name (maximum 255 ASCII characters, including spaces) Note: If **Peer ID Type** is **IP**, please read the rest of this section. If you type 0.0.0.0, the ZyWALL uses the IP address specified in the **Secure Gateway Address** field. This is not recommended in the following situations: • There is a NAT router between the ZyWALL and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Peer ID Type**.
Extended Authentication	
Enable Extended Authentication	Select this if one of the routers (the ZyWALL or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server.
Server Mode	Select this if the ZyWALL authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the ZyWALL authenticates this information.
Client Mode	Select this radio button if the ZyWALL provides a username and password to the remote IPSec router for authentication. You also have to provide the **User Name** and the **Password**.
User Name	This field is required if the ZyWALL is in **Client Mode** for extended authentication. Type the user name the ZyWALL sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the ZyWALL is in **Client Mode** for extended authentication. Type the password the ZyWALL sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.

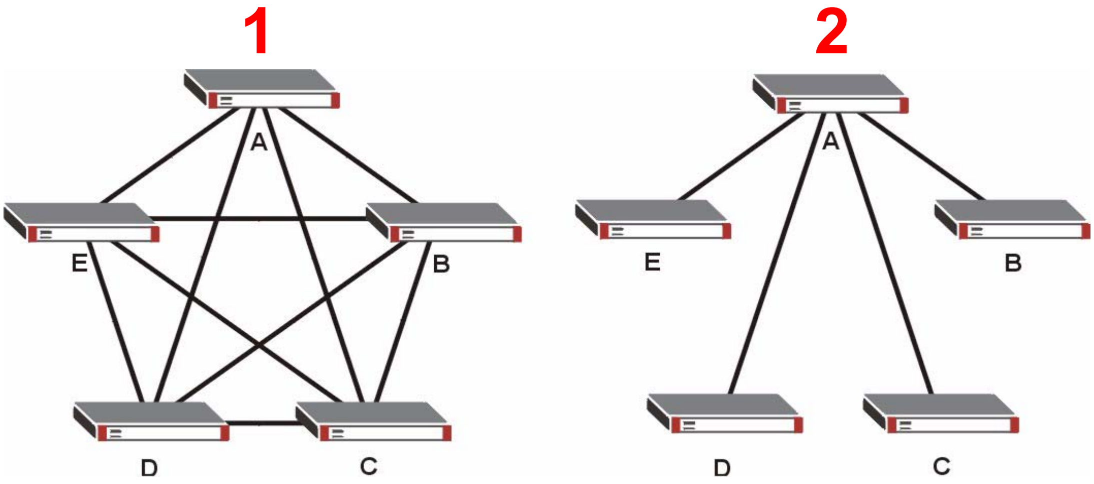
Table 96 VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes in the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

20.5 VPN Concentrator

A VPN concentrator combines several VPN connections into one secure network. Figure 207 on page 318 shows an example of this, as well as one alternative approach.

Figure 207 VPN Topologies



The VPN concentrator is used in the second approach. In the first (fully-meshed) approach, there is a VPN connection between every pair of routers. In the second (hub-and-spoke) approach, there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

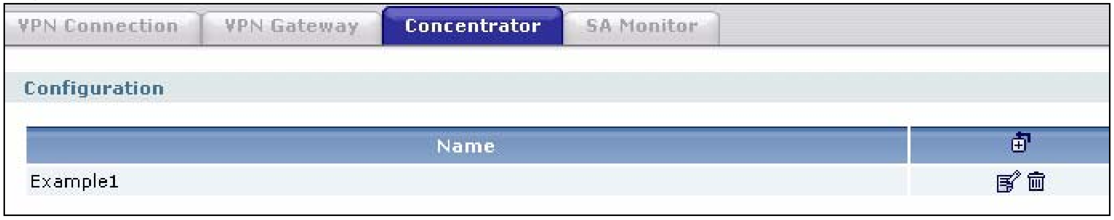
The biggest advantage of a VPN concentrator is that it reduces the number of VPN connections that you have to set up and maintain in the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

You should not use a VPN concentrator in every situation, however. The hub router is a single point of failure, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). In addition, there is a significant burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

20.5.1 VPN Concentrator Summary

You use the **VPN Concentrator** summary screen to look at the VPN concentrators you have set up. The **VPN Concentrator** summary screen displays the VPN concentrators in the ZyWALL. To access this screen, click **VPN** > **IPSec VPN** > **Concentrator**. The following screen appears.

Figure 208 VPN > IPSec VPN > Concentrator



Example1

Each field is discussed in the following table. See Section 20.5.2 on page 319 for more information.

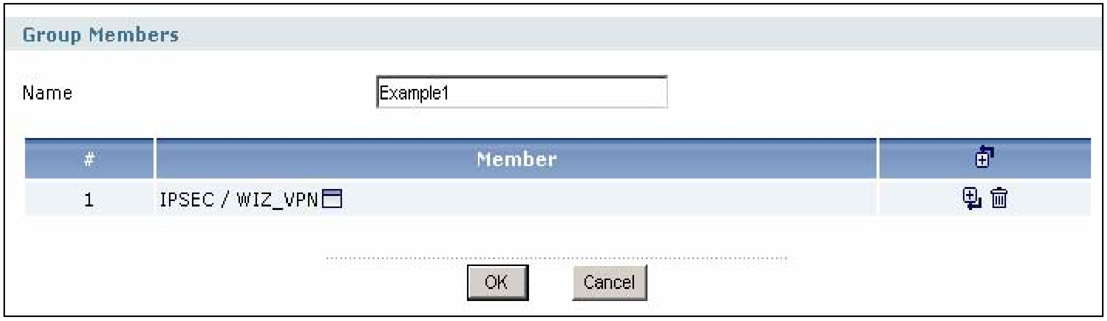
Table 97 VPN > IPSec VPN > Concentrator

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific concentrator.
Name	This field displays the name of the VPN concentrator.
Add icon	This column provides icons to add, edit, and remove VPN concentrators. To add a VPN concentrator, click the **Add** icon at the top of the column. The **VPN Concentrator Add/Edit** screen appears. To edit a VPN concentrator, click the **Edit** icon next to the concentrator. The **VPN Concentrator Add/Edit** screen appears accordingly. To delete a VPN concentrator, click on the **Remove** icon next to the concentrator. The web configurator confirms that you want to delete the VPN concentrator.

20.5.2 VPN Concentrator Add/Edit

The **VPN Concentrator Add/Edit** screen allows you to create a new VPN concentrator or edit an existing one. To access this screen, go to the **VPN Concentrator** summary screen (see Section 20.5.1 on page 319), and click either the **Add** icon or an **Edit** icon.

Figure 209 VPN > IPSec VPN > Concentrator > Edit

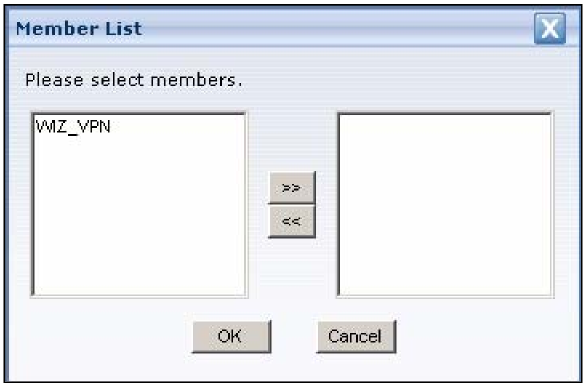


Name: Example1

1 IPSEC / WIZ_VPN

Each field is described in the following table.

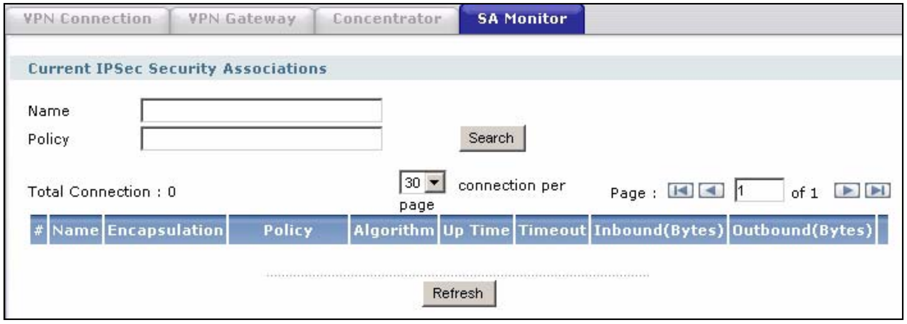
Table 98 VPN > IPSec VPN > Concentrator > Edit

LABEL	DESCRIPTION
Name	Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
#	This field is a sequential value, and it is not associated with a specific member in the concentrator.
Member	This field displays the name of each member in the concentrator. Note: You must disable policy enforcement in each member. See Section 20.3.2 on page 298. Click the **Popup** icon to change this member in the group. The following screen appears. **Figure 210** Network > IPSec VPN > Concentrator > Edit > Member  Member List Please select members. WIZ_VPN >> << OK Cancel
Add icon	This column provides icons to add members to and remove members from the concentrator. To add a member to the concentrator, click the **Add** icon at the top of the column to add the new member at the beginning of the list, or click the **Add** icon next to an existing member to add the new member after the existing one. The web configurator chooses a new member alphabetically. You can use the **Popup** icon next to the new member to change this. To remove a member from the concentrator, click on the **Remove** icon next to the member. The web configurator confirms that you want to remove the member.
OK	Click **OK** to save your changes in the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

20.6 SA Monitor Screen

You can use the **SA Monitor** screen to display and to manage active IPSec SA. To access this screen, click **VPN** > **IPSec VPN** > **SA Monitor**. The following screen appears.

Figure 211 VPN > IPSec VPN > SA Monitor


VPN Connection
VPN Gateway
Concentrator
SA Monitor
Current IPSec Security Associations
Name
Policy
Search
# | Name | Encapsulation | Policy | Algorithm | Up Time | Timeout | Inbound(Bytes) | Outbound(Bytes)
Refresh

Total Connection : 0

30 connection per page

Page : 1 of 1

Each field is described in the following table.

Table 99 VPN > IPSec VPN > SA Monitor

LABEL	DESCRIPTION
Name	Enter the name of a IPSec SA here and click **Search** to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 20.6.1 on page 322 for more details.
Policy	Enter the IP address(es) or names of the local and remote policies for an IPSec SA and click **Search** to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 20.6.1 on page 322 for more details.
Search	Click this button to search for an IPSec SA that matches the information you specified above.
Total Connection	This field displays the total number of associated IPSec SAs.
connection per page	Select how many entries you want to display on each page.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Policy	This field displays the content of the local and remote policies for this IPSec SA. The IP addresses, not the address objects, are displayed.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Up Time	This field displays how many seconds the IPSec SA has been active. This field displays **N/A** if the IPSec SA uses manual keys.
Timeout	This field displays how many seconds remain in the SA life time, before the ZyWALL automatically disconnects the IPSec SA. This field displays **N/A** if the IPSec SA uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the ZyWALL since the IPSec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the ZyWALL to the remote IPSec router since the IPSec SA was established.
Disconnect	This field is displayed if the IPSec SA does not use manual keys. Click the **Disconnect** icon next to an IPSec SA to disconnect it.
Refresh	Click **Refresh** to update the information in the display.

20.6.1 Regular Expressions in Searching IPSec SAs by Name or Policy

A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.

Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use “*abc” (without the quotation marks) to specify any VPN connection or policy name that ends with “abc”. A VPN connection named “testabc” would match. There could be any number (of any type) of characters in front of the “abc” at the end and the VPN connection or policy name would still match. A VPN connection or policy name named “testacc” for example would not match.

A * in the middle of a VPN connection or policy name has the ZyWALL check the beginning and end and ignore the middle. For example, with “abc*123”, any VPN connection or policy name starting with “abc” and ending in “123” matches, no matter how many characters are in between.

The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

21

SSL VPN

This chapter shows you how to set up secure SSL VPN access for remote user login. See Section 5.4.5 on page 116 for related information on these screens.

21.1 SSL Access Policy

An SSL access policy allows the ZyWALL to perform the following tasks:

- limit user access to specific applications or files on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

21.1.1 SSL Access Policy Objects

Your ZyWALL uses the object-based configuration approach in which related settings are grouped into an object. Once you have set up an object, you can apply and reuse it in other configuration screens. Thus, the object-based approach minimizes repetitive configuration steps and helps to reduce management and configuration efforts.

Objects store information and are referenced in the **SSL Access Privilege** screen. If you update this information, in response to changes, the ZyWALL automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

The following table gives an overview of the settings you can configure in the corresponding **Object** screens or through the **SSL Access Privilege** screen.

Table 100 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Configure a user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Configure an SSL application object to specify the application type and server users are allowed to access.
IP Pool	Address	Configure an address object that defines a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.

Table 100 Objects (continued)

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
Server Addresses	Address	Configure address objects for the IP addresses of the DNS and WINS servers that the ZyWALL sends to the VPN connection users.
VPN Network	Address	Configure an address object to specify which network segment users are allowed to access through a VPN connection.

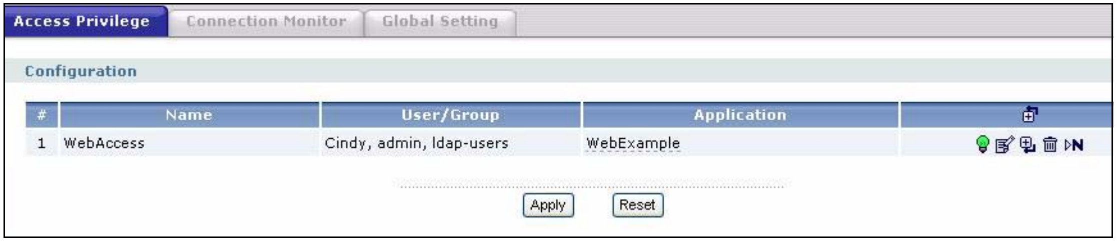
21.1.2 SSL Access Policy Limitations

You cannot delete an object that is used by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

21.2 SSL Access Privilege List

Click **VPN** > **SLL VPN** to open the **Access Privilege** screen. This screen displays a summary of the SSL access policy(ies) you have configured.

Figure 212 VPN > SSL VPN > Access Privilege



#	Name	User/Group	Application
1	WebAccess	Cindy, admin, ldap-users	WebExample

The following table describes the labels in this screen.

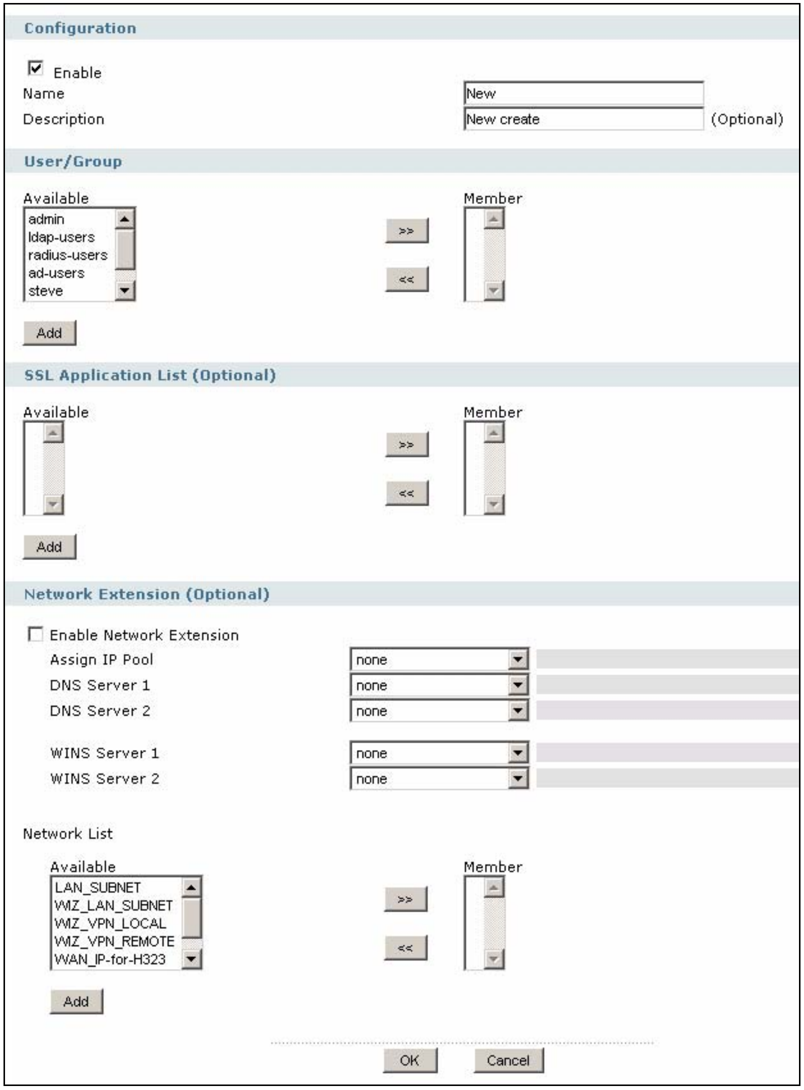
Table 101 VPN > SSL VPN > Access Privilege

LABEL	DESCRIPTION
#	This field displays the index number of the entry.
Name	This field displays the descriptive name of the SSL access policy for identification purposes.
User/Group	This field displays the user account or user group name(s) associated to an SSL access policy. This field displays up to three names.
Application	This field displays the descriptive name of the SSL application object this policy uses.
Add icon	This column provides icons to add, edit, and remove policies. To add a new policy, click the **Add** icon at the top of the column. To activate or disable the policy, click the **Activate**/**Deactivate** icon. To edit a policy, click the **Edit** icon next to the policy. To delete a policy, click the **Remove** icon next to the policy. To rearrange a policy in the list, click the **Move to N** icon next to the policy.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to discard all changes.

21.3 Creating/Editing an SSL Access Policy

To create a new or edit an existing SSL access policy, click the **Add** or **Edit** icon in the **Access Privilege** screen.

Figure 213 VPN > SSL VPN > Access Privilege > Add/Edit



Configuration

☑ Enable

Name: New

Description: New create (Optional)

User/Group

Available: admin, ldap-users, radius-users, ad-users, steve

SSL Application List (Optional)

Network Extension (Optional)

☐ Enable Network Extension

Assign IP Pool: none

DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

Network List

Available: LAN_SUBNET, WIZ_LAN_SUBNET, WIZ_VPN_LOCAL, WIZ_VPN_REMOTE, WAN_IP-for-H323

The following table describes the labels in this screen.

Table 102 VPN > SSL VPN > Access Privilege > Add/Edit

LABEL	DESCRIPTION
Configuration	
Enable	Select this option to activate this SSL access policy.
Name	Enter a descriptive name to identify this policy. You can enter up to 15 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed.
Description	Enter additional information about this SSL access policy. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”).

Table 102 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
User/Group	The **Available** list displays the name(s) of the user account and/or user group(s) to which you have not applied an SSL access policy yet. To associate a user or user group to this SSL access policy, select a user account or user group and click **>>** to add to the **Member** list. You can select more than one name. To remove a user or user group, select the name(s) in the **Member** list and click **<<**.
Add	Click **Add** to display a screen you use to create a new user account or user group name (see Section 34.2.1 on page 506 for details).
SSL Application List	The **Available** list displays the name(s) of the SSL application(s) you can select for this SSL access policy. To associate an SSL application to this SSL access policy, select a name and click **>>** to add to the **Member** list. You can select more than one application. To remove an SSL application, select the name(s) in the **Member** list and click **<<**.
Add	Click **Add** to create a new SSL application object. Refer to Section 42.3 on page 568 for more information.
Network Extension	
Enable Network Extension	Select this option to create a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network. Clear this option to disable this feature. Users can only access the applications as defined by the selected SSL application settings and the remote user computers are not made to be a part of the local network.
Assign IP Pool	Define a separate pool of IP addresses to assign to the SSL users. Select it here. The SSL VPN IP pool cannot overlap with IP addresses on the ZyWALL's local networks (LAN and DMZ for example), the SSL user's network, or the networks you specify in the SSL VPN **Network List**.
DNS/WINS Server 1..2	Select the name of the DNS or WINS server whose information the ZyWALL sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.
Network List	To allow user access to local network(s), select a network name in the **Available** list and click **>>** to add to the **Member** list. You can select more than one network. To block access to a network, select the network name in the **Member** list and click **<<**.
Add	Click **Add** to create a new network object. Refer to Chapter 35 on page 515 for more information.
Ok	Click **Ok** to save the changes and return to the main **Access Privilege** screen.
Cancel	Click **Cancel** to discard all changes and return to the main **Access Privilege** screen.

21.4 SSL Connection Monitor

The ZyWALL keeps track of the users who are currently logged into the VPN SSL client portal. Click **VPN > SSL VPN** in the navigation panel and click the **Connection Monitor** tab to display the user list.

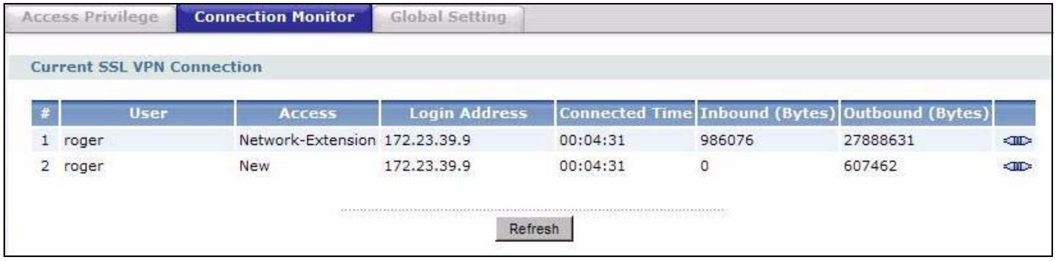
Use this screen to do the following:

- view a list of users currently logged in through VPN SSL.

- log out a user and delete related session information.

Once a user logs out, the corresponding entry is removed from the **Connection Monitor** screen.

Figure 214 VPN > SSL VPN > Connection Monitor



Current SSL VPN Connection

#	User	Access	Login Address	Connected Time	Inbound (Bytes)	Outbound (Bytes)	
1	roger	Network-Extension	172.23.39.9	00:04:31	986076	27888631	
2	roger	New	172.23.39.9	00:04:31	0	607462	

The following table describes the labels in this screen.

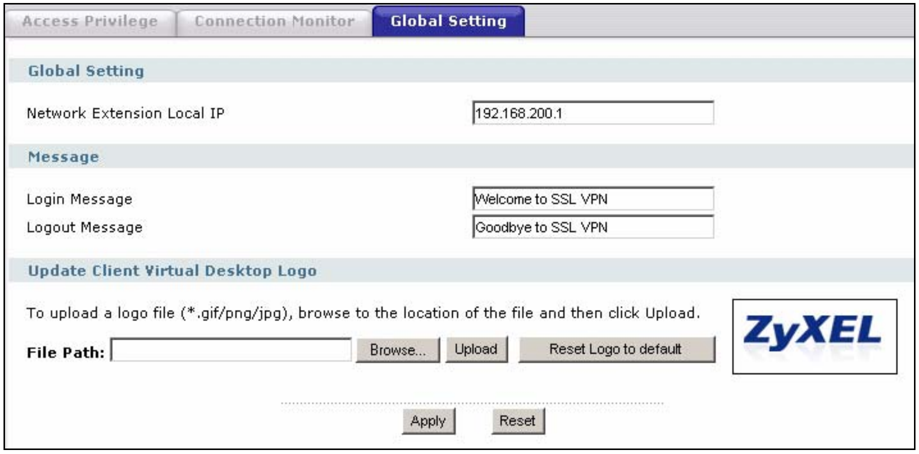
Table 103 VPN > SSL VPN > Connection Monitor

LABEL	DESCRIPTION
#	This field displays the index number.
User	This field displays the account user name used to establish this SSL VPN connection.
Access	This field displays the name of the SSL VPN application the user is accessing.
Login Address	This field displays the IP address the user used to establish this SSL VPN connection.
Connected Time	This field displays the time this connection was established.
Inbound (Bytes)	This field displays the number of bytes received by the ZyWALL on this connection.
Outbound (Bytes)	This field displays the number of bytes transmitted by the ZyWALL on this connection.
	Click the icon to terminate the connection of the user and delete corresponding session information from the ZyWALL.
Refresh	Click **Refresh** to update this screen.

21.5 Configuring SSL Global Setting

Click **VPN > SSL VPN** and click the **Global Setting** tab to display the configuration screen. Use this screen to set the IP address of the ZyWALL (or a gateway device) on your network, enter access messages or upload a custom logo to be displayed on the remote user screen.

Figure 215 VPN > SSL VPN > Global Setting



Network Extension Local IP: 192.168.200.1

Login Message: Welcome to SSL VPN

Logout Message: Goodbye to SSL VPN

To upload a logo file (*.gif/png/jpg), browse to the location of the file and then click Upload.

File Path:

The following table describes the labels in this screen.

Table 104 VPN > SSL VPN > Global Setting

LABEL	DESCRIPTION
Global Setting	
Network Extension IP Address	Specify the IP address of the ZyWALL (or a gateway device) for full tunnel mode SSL VPN access. Leave this field to the default settings unless it conflicts with another interface.
Message	
Login Message	Specify a message to display on the screen when a user logs in and an SSL VPN connection is established successfully. You can enter up to 31 characters (“a-z”, A-Z”, “0-9”) with spaces allowed.
Logout Message	Specify a message to display on the screen when a user logs out and the SSL VPN connection is terminated successfully. You can enter up to 31 characters (“a-z”, A-Z”, “0-9”) with spaces allowed.
Update Client Virtual Desktop Logo	You can upload a graphic logo to be displayed on the web browser on the remote user computer. The ZyXEL company logo is the default logo. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 127 x 57 pixels to avoid distortion when displayed. The ZyWALL automatically resizes a graphic of a different resolution to 127 x 57 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.
Browse	Click **Browse** to locate the graphic file on your computer.
Upload	Click **Upload** to transfer the specified graphic file from your computer to the ZyWALL.
Reset Logo to Default	Click **Reset Logo to Default** to display the ZyXEL company logo on the remote user’s web browser.
Apply	Click **Apply** to save the changes and/or start the logo file upload process.
Reset	Click **Reset** to start configuring this screen again.

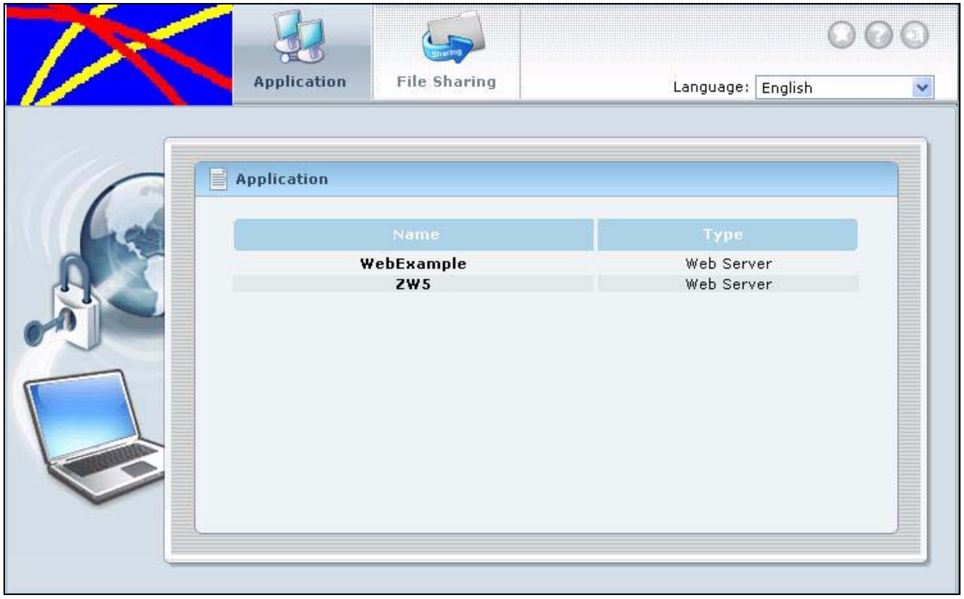
21.5.1 Uploading a Custom Logo

Follow the steps below to upload a custom logo on the ZyWALL.

1. Click **VPN** > **SSL VPN** and click the **Global Setting** tab to display the configuration screen.
2. Click **Browse** to locate the logo graphic. Make sure the file is in GIF format.
3. Click **Apply** to start the file transfer process.
4. Log in as a user to verify that the new logo displays properly.

The following shows an example logo on the remote user screen.

Figure 216 Example Logo Graphic Display



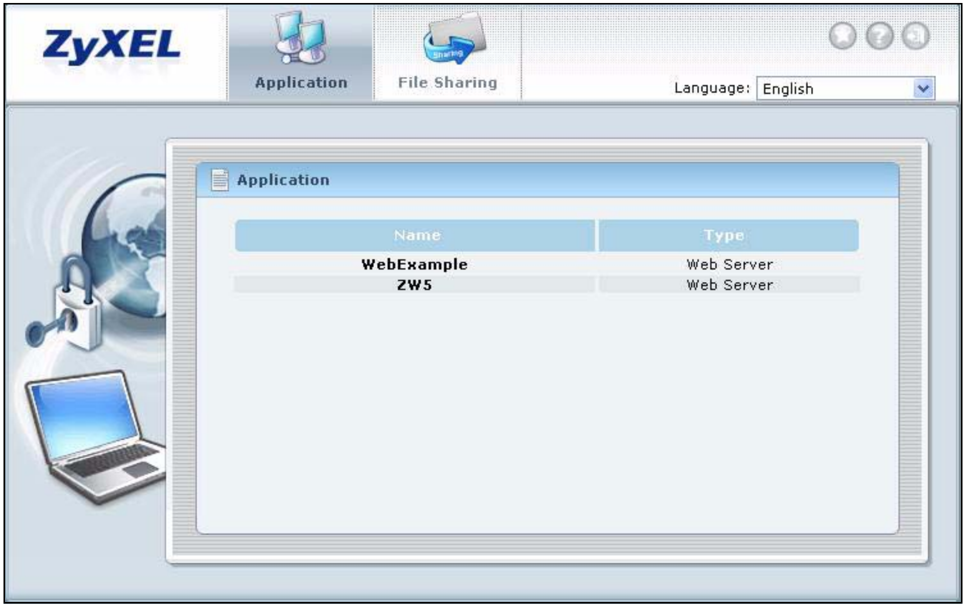
Name	Type
WebExample	Web Server
ZW5	Web Server

21.6 Establishing an SSL VPN Connection

Follow the steps below to establish an SSL VPN connection.

1. Display the login screen and enter your user account information (the user name and password).
2. Select **Login to SSL VPN**.
3. Click **Login**.
4. SSL VPN connection starts. This may take several minutes depending on your network connection. Once the connection is up, you should see the client portal screen. The following shows an example.

Figure 217 SSL VPN Client Portal Screen Example


ZyXEL
Application
File Sharing
Language:
English
Application

Name	Type
WebExample	Web Server
ZW5	Web Server

If the user account is not set up for SSL VPN access, an “SSL VPN connection is not activated” message displays in the **Login** screen. Clear the **Login to SSL VPN** check box and try logging in again.

For more information on user portal screens, refer to Chapter 22 on page 331.

22

SSL User Screens

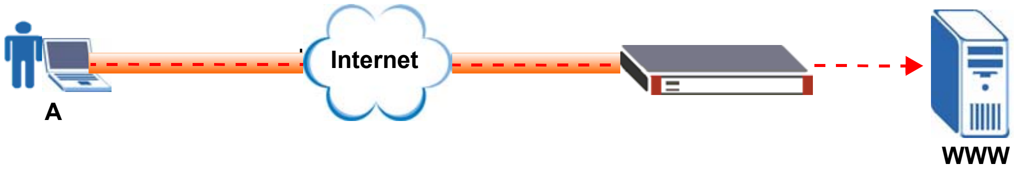
This chapter introduces secure network access and gives an overview of the remote user screens on the ZyWALL.

22.1 Overview

The ZyWALL provides secure connections to network resources such as applications, files, intranet sites or e-mail through a web-based interface and using Microsoft Outlook Web Access (OWA).

The following figure shows a network example where a remote user (**A**) logs into the ZyWALL from the Internet to access the web server (**WWW**) on the local network.

Figure 218 Network Example



22.1.1 Network Resource Access Methods

As a remote user, you can access resources on the local network using one of the following methods.

- Using a supported web browser
  Once you have successfully logged in through the ZyWALL, you can access any intranet site, web-based applications or web-based e-mails using one of the supported web browsers.
- Using the Java thin clients
  The ZyWALL automatically loads Java thin client programs to your computer after a successful login. With the thin clients, you can access servers, remote desktops and manage files as if you were on the local network.

22.1.2 System Requirements

The following lists the browser and computer system requirements for remote user access.

- Windows 2000 and Windows XP

- Internet Explorer 5.5 and above (for IE7, JRE 1.6 must be enabled)
- Netscape 7.2 and above
- Firefox 1.0 and above
- Mozilla 1.7.3 and above
- Sun Java Virtual Machine (JVM) installed with a minimum version of 1.4.
- Java enabled in Internet Explorer on Windows computers.

22.1.3 Information You Need

Your network administrator should provide the following information that allows you to log in and access network resources.

- the domain name or IP address of the ZyWALL
- the login account user name and password
- if also required, the user name and/or password to access the network resource

22.1.4 Certificates

Your computer establishes an HTTPS connection to the ZyWALL to access the login screen. If instructed by your network administrator, you must install or import a certificate (provided by the ZyWALL or your network administrator).

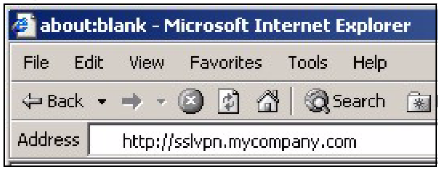
Refer to Appendix E on page 713 for more information.

22.2 Remote User Login

This section shows you how to access and log into the network through the ZyWALL. Example screens for Internet Explorer are shown.

1 Open a web browser and enter the web site address or IP address of the ZyWALL. For example, “http://sslvpn.mycompany.com”.

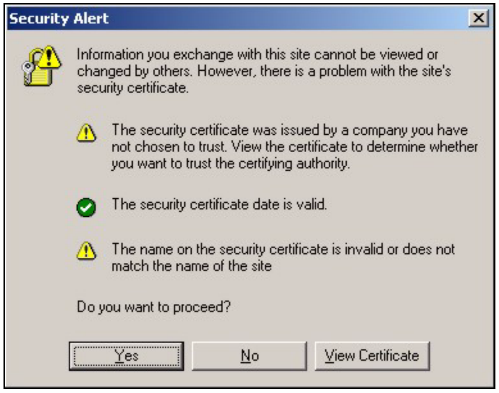
Figure 219 Enter the Address in a Web Browser



Address: http://sslvpn.mycompany.com

2 Click **OK** or **Yes** if a security screen displays.

Figure 220 Login Security Screen



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

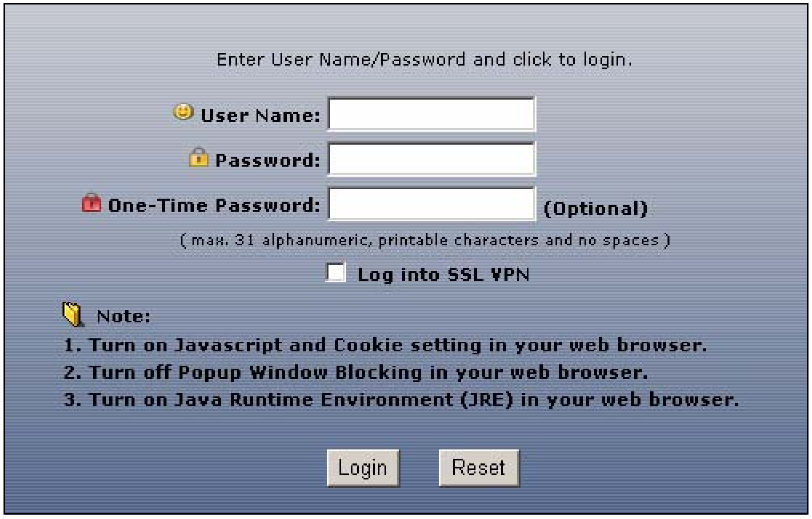
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

3 A login screen displays. Enter the user name and password of your login account. If a token password is also required, enter it in the **One-Time Password** field.

4 Select **Log into SSL VPN** and click **Login** to log in and establish an SSL VPN connection to the network to access network resources.

Figure 221 Login Screen



Enter User Name/Password and click to login.

User Name:

Password:

One-Time Password: (Optional)

(max. 31 alphanumeric, printable characters and no spaces)

☐ Log into SSL VPN

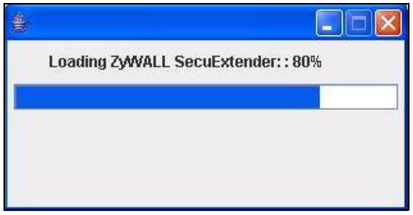
Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

5 Your computer starts establishing a secure connection to the ZyWALL after a successful login. This may take up to two minutes. If a warning screen displays, click **OK**, **Yes** or **Continue**.

6 The following status screen displays indicating the progress of the secure SSL VPN connection setup.

Figure 222 SecuExtender Progress



Loading ZyWALL SecuExtender: : 80%

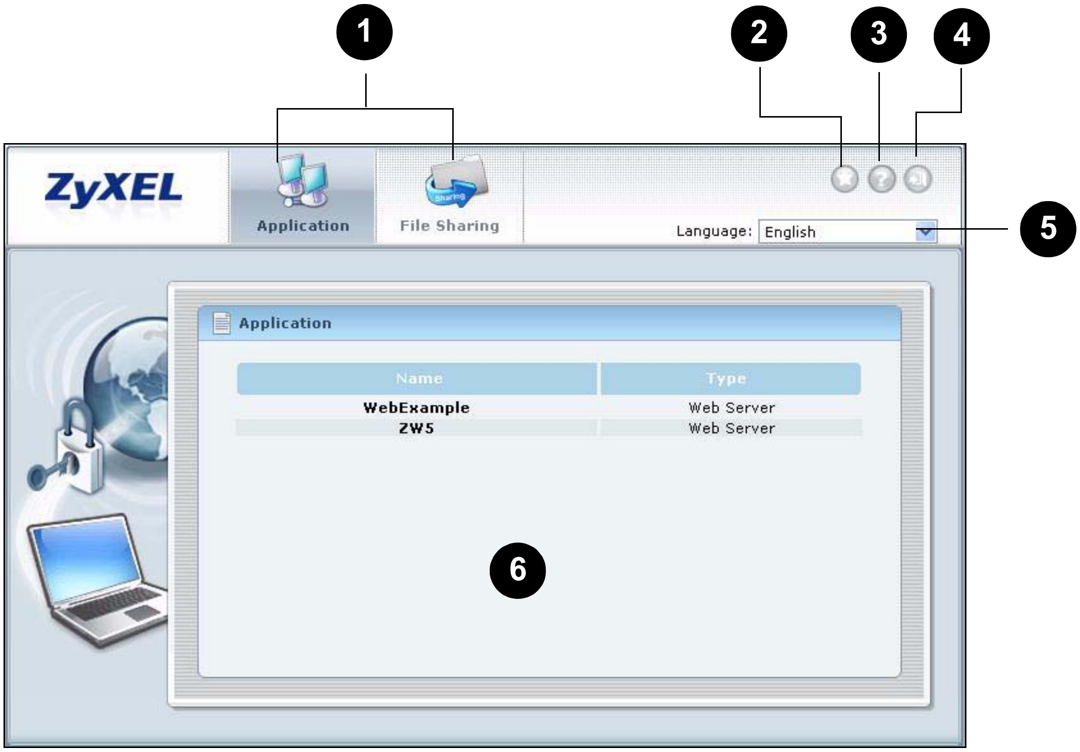
7 The **Application** screen displays showing the list of resources available to you. See Figure 223 on page 334 for a screen example.

Available resource links vary depending on the configuration your network administrator made.

22.3 SSL VPN User Screens

This section describes the main elements in the remote user screens.

Figure 223 Remote User Screen



Name	Type
WebExample	Web Server
ZW5	Web Server

The following table describes the various parts of a remote user screen.

Table 105 Remote User Screen Overview

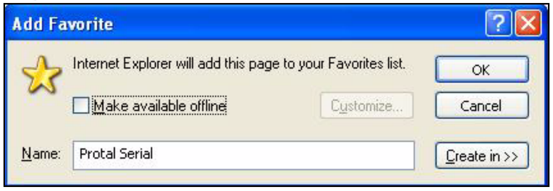
#	DESCRIPTION
1	Click on a menu tab to go to the **Application** or **File Sharing** screen.
2	Click this icon to create a bookmark to the SSL VPN user screen in your web browser.
3	Click this icon to display the on-line help window.
4	Click this icon to log out and terminate the secure connection.
5	Select your preferred language for the interface.
6	This part of the screen displays a list of the resources available to you. In the **Application** screen, click on a link to access or display the access method. In the **File Sharing** screen, click on a link to open a file or directory.

22.4 Bookmark

You can create a bookmark of the ZyWALL by clicking the **Add to Favorite** icon. This allows you to access the ZyWALL using the bookmark without having to enter the address every time.

1. In any remote user screen, click the **Add to Favorite** icon.
2. A screen displays. Accept the default name in the **Name** field or enter a descriptive name to identify this link.
3. Click **OK** to create a bookmark in your web browser.

Figure 224 Add Favorite



Internet Explorer will add this page to your Favorites list.

☐ Make available offline

Name: Protal Serial

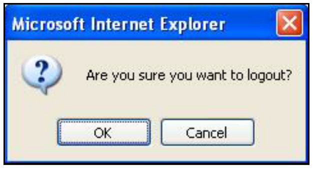
22.5 Logout

To properly terminate a connection, click on the **Logout** icon in any remote user screen.

The login screen, history information in your browser cache is also erased once you log out.

1. Click the **Logout** icon in any remote user screen.
2. A prompt window displays. Click **OK** to continue.

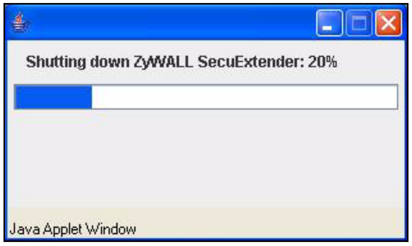
Figure 225 Logout: Prompt



Are you sure you want to logout?

3. An information screen displays to indicate that the SSL VPN connection is about to terminate.

Figure 226 Logout: Connection Termination Progress



Shutting down ZyWALL SecuExtender: 20%

23

SSL User Application Screens

This chapter describes the **Application** screens you use to access an application on the network through the SSL VPN connection.

23.1 Overview

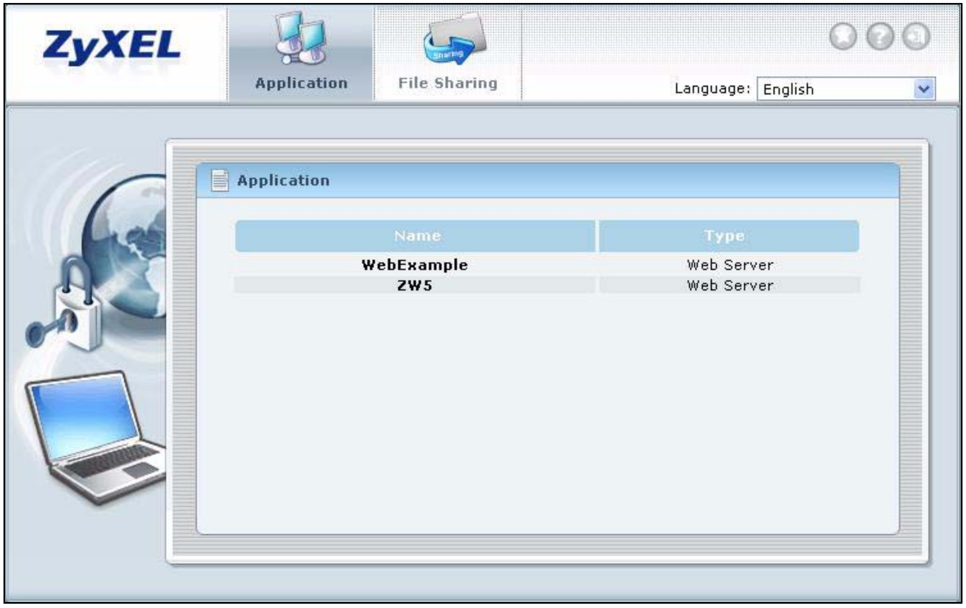
Depending on the configuration of your network administrator, you can use the **Application** screen to access web-based applications (such as web sites and e-mail).

23.1.1 The Application Screen

Click the **Application** tab to display the screen. The **Name** field displays the descriptive name for an application. The **Type** field displays wether the application is a web site (**Web Server**) or web-based e-mail using Microsoft Outlook Web Access (**OWA**).

To access a web-based application, simply click a link in the **Application** screen to display the web screen in a separate browser window.

Figure 227 Application



Name	Type
WebExample	Web Server
ZW5	Web Server

24

SSL User File Sharing Screens

This chapter describes the **File Sharing** screen you use to access files on a file server through the SSL VPN connection.

24.1 Overview

Use the **File Sharing** screen to display and access shared files/folders on a file server.

You can also perform the following actions:

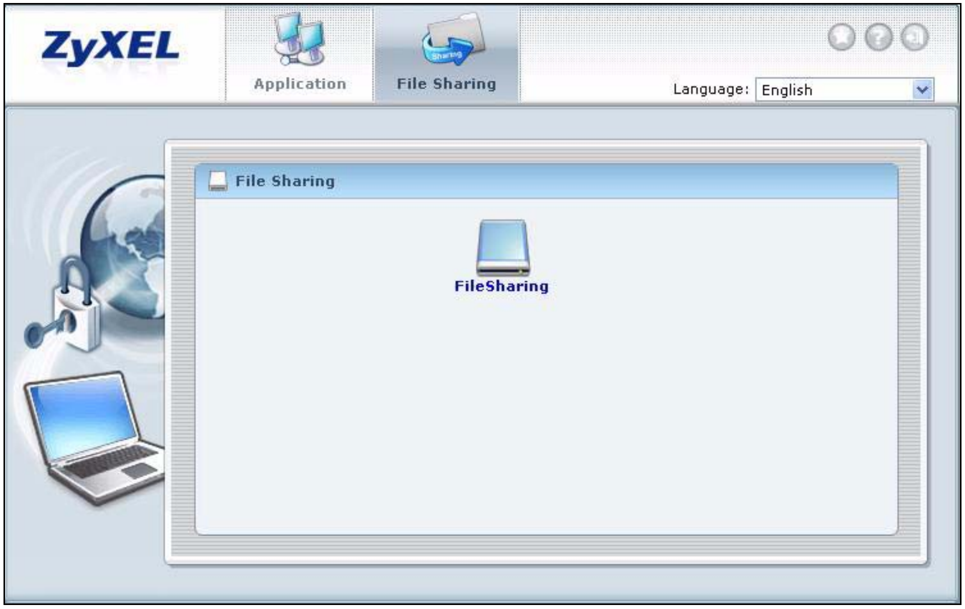
- Access a folder.
- Open a file (if your web browser cannot open the file, you are prompted to download it).
- Save a file to your computer.
- Create a new folder.
- Rename a file or folder.
- Delete a file or folder.
- Upload a file.

Available actions you can perform in the **File Sharing** screen vary depending on the rights granted to you on the file server.

24.2 Main File Sharing Screen

The first **File Sharing** screen displays the name(s) of the shared folder(s) available. The following figure shows an example with one file share.

Figure 228 File Sharing

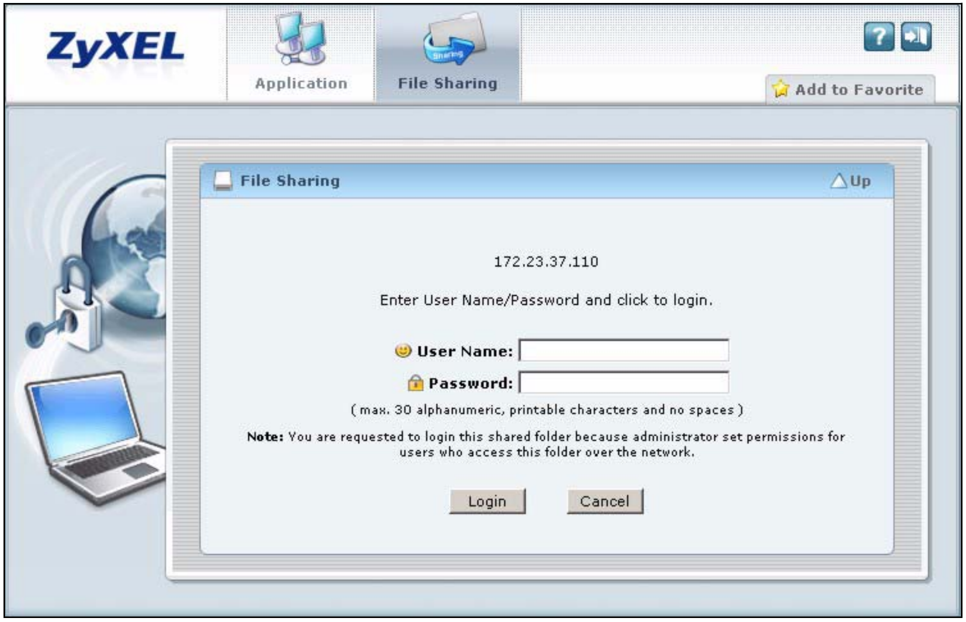

ZyXEL
Application
File Sharing
Language: English
File Sharing
FileSharing

24.3 Opening a File or Folder

You can open a file if the file extension is recognized by the web browser and the associated application is installed on your computer.

1. Log in as a remote user and click the **File Sharing** tab.
2. Click on a file share icon.
3. If an access user name and password are required, a screen displays as shown in the following figure. Enter the account information and click **Login** to continue.

Figure 229 File Sharing: Enter Access User Name and Password


ZyXEL
Application
File Sharing
Add to Favorite
File Sharing
Up
Login
Cancel

172.23.37.110

Enter User Name/Password and click to login.

User Name:
Password:

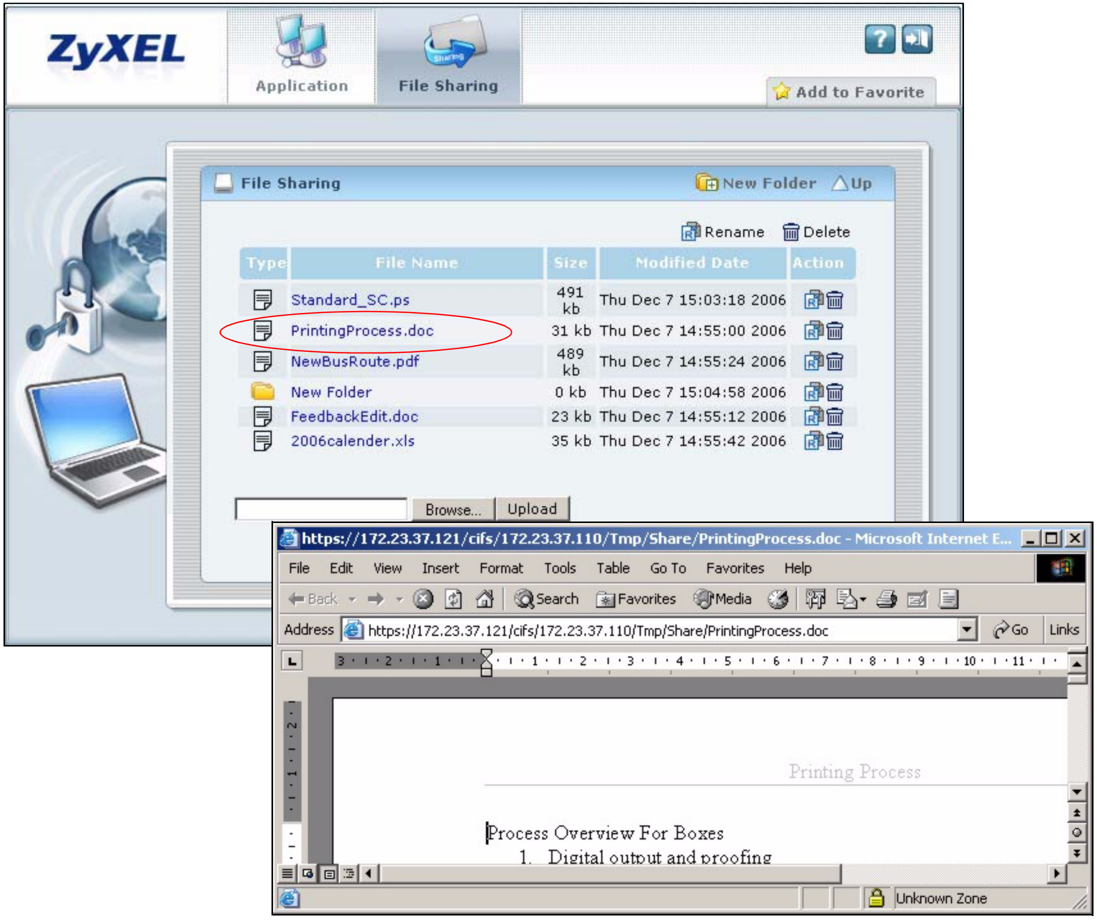
(max. 30 alphanumeric, printable characters and no spaces)

Note: You are requested to login this shared folder because administrator set permissions for users who access this folder over the network.

4 A list of files/folders displays. Click on a file to open it in a separate browser window. You can also click a folder to access it.

For this example, click on a .doc file to open the Word document.

Figure 230 File Sharing: Open a Word File


ZyXEL
Application
File Sharing
Add to Favorite
File Sharing
New Folder
Up
Rename
Delete
Browse...
Upload
https://172.23.37.121/cifs/172.23.37.110/Tmp/Share/PrintingProcess.doc - Microsoft Internet E...
File
Edit
View
Insert
Format
Tools
Table
Go To
Favorites
Help
Back
Search
Favorites
Media
Address
https://172.23.37.121/cifs/172.23.37.110/Tmp/Share/PrintingProcess.doc
Go
Links
Unknown Zone

Type	File Name	Size	Modified Date	Action
	Standard_SC.ps	491 kb	Thu Dec 7 15:03:18 2006	
	PrintingProcess.doc	31 kb	Thu Dec 7 14:55:00 2006	
	NewBusRoute.pdf	489 kb	Thu Dec 7 14:55:24 2006	
	New Folder	0 kb	Thu Dec 7 15:04:58 2006	
	FeedbackEdit.doc	23 kb	Thu Dec 7 14:55:12 2006	
	2006calender.xls	35 kb	Thu Dec 7 14:55:42 2006	

Printing Process

Process Overview For Boxes

1. Digital output and proofing

24.3.1 Downloading a File

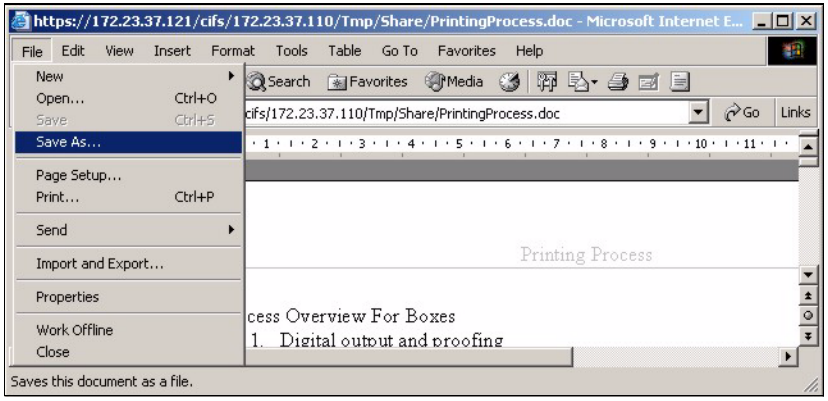
You are prompted to download a file which cannot be opened using a web browser.

Follow the on-screen instructions to download and save the file to your computer. Then launch the associated application to open the file.

24.3.2 Saving a File

After you have opened a file in a web browser, you can save a copy of the file by clicking **File > Save As** and following the on-screen instructions.

Figure 231 File Sharing: Save a Word File


https://172.23.37.121/cifs/172.23.37.110/Tmp/Share/PrintingProcess.doc - Microsoft Internet E...
File
Edit
View
Insert
Format
Tools
Table
Go To
Favorites
Help
New
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Send
Import and Export...
Properties
Work Offline
Close
Search
Favorites
Media
cifs/172.23.37.110/Tmp/Share/PrintingProcess.doc
Go
Links
Printing Process
cess Overview For Boxes
1. Digital output and proofing

Saves this document as a file.

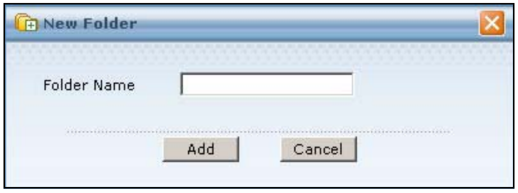
24.4 Creating a New Folder

To create a new folder in the file share location, click the **New Folder** icon.

Specify a descriptive name for the folder. You can enter up to 356 characters. Then click **Add**.

Make sure the length of the folder name does not exceed the maximum allowed on the file server.

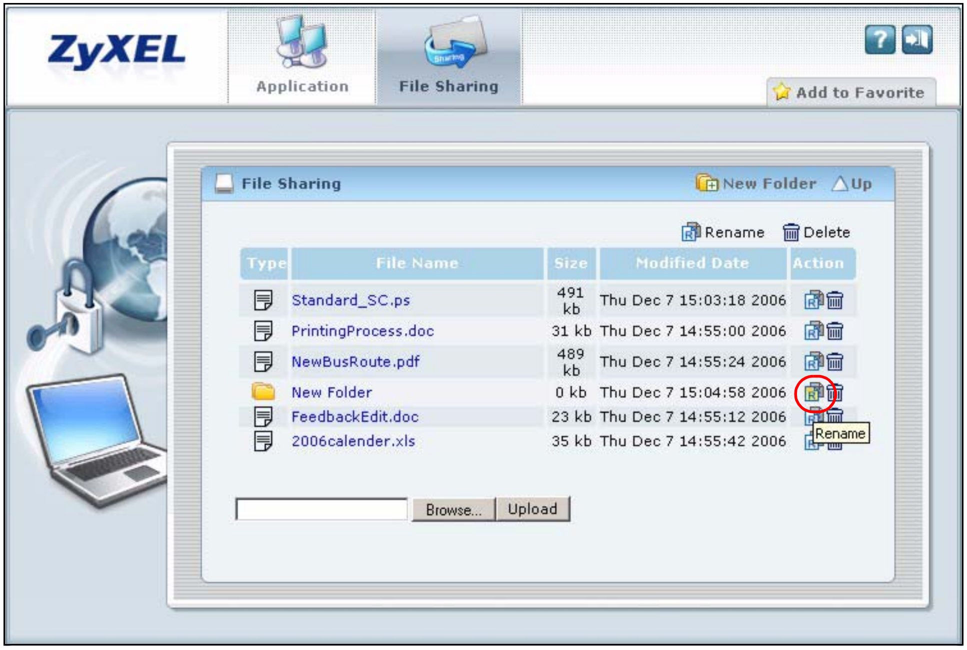
Figure 232 File Sharing: Save a Word File


New Folder
Folder Name
Add
Cancel

24.5 Renaming a File or Folder

To rename a file or folder, click the **Rename** icon next to the file/folder.

Figure 233 File Sharing: Rename


ZyXEL
Application
File Sharing
Add to Favorite
File Sharing
New Folder
Up
Rename
Delete
Rename
Browse...
Upload

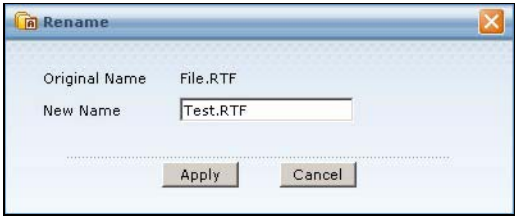
Type	File Name	Size	Modified Date	Action
	Standard_SC.ps	491 kb	Thu Dec 7 15:03:18 2006	
	PrintingProcess.doc	31 kb	Thu Dec 7 14:55:00 2006	
	NewBusRoute.pdf	489 kb	Thu Dec 7 14:55:24 2006	
	New Folder	0 kb	Thu Dec 7 15:04:58 2006	
	FeedbackEdit.doc	23 kb	Thu Dec 7 14:55:12 2006	
	2006calender.xls	35 kb	Thu Dec 7 14:55:42 2006	

A popup window displays. Specify the new name and/or file extension in the field provided. You can enter up to 356 characters. Then click **Apply**.

Make sure the length of the name does not exceed the maximum allowed on the file server.

You may not be able to open a file if you change the file extension.

Figure 234 File Sharing: Rename

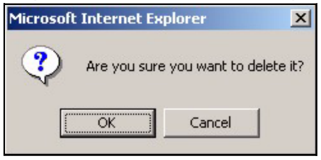

Rename
Apply
Cancel

Original Name File.RTF
New Name Test.RTF

24.6 Deleting a File or Folder

To delete a file or folder, click the **Delete** icon next to the file/folder and then OK in a prompt screen that displays.

Figure 235 File Sharing: Delete Prompt


Microsoft Internet Explorer
OK
Cancel

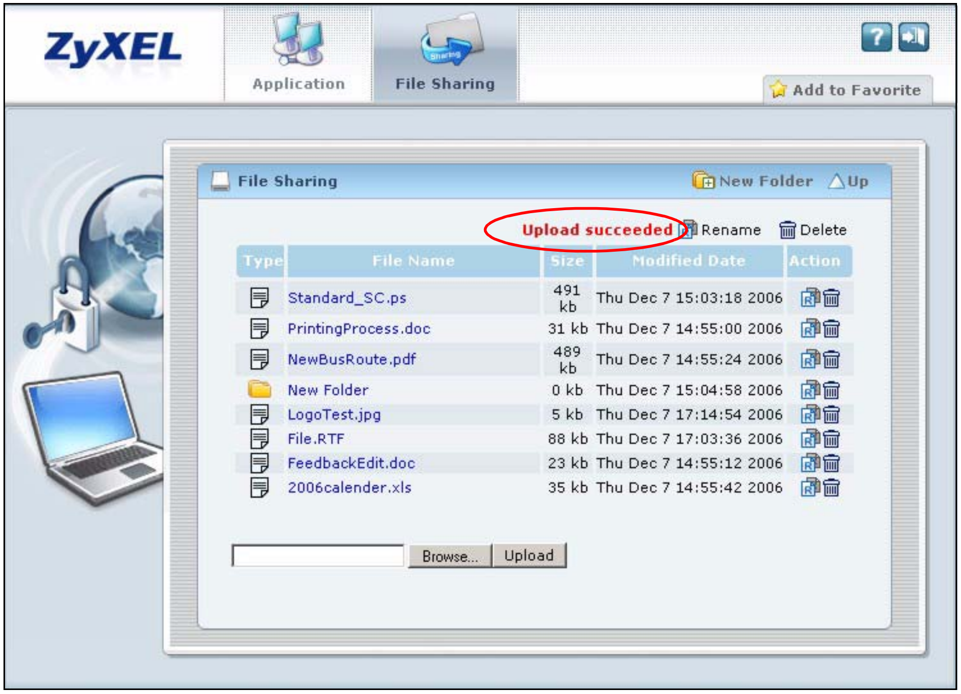
Are you sure you want to delete it?

24.7 Uploading a File

Follow the steps below to upload a file to the file server.

1. Log into the remote user screen and click the **File Sharing** tab.
2. Specify the location and/or name of the file you want to upload. Or click **Browse** to locate it.
3. Click **Upload** to send the file to the file server.
4. After the file is uploaded successfully, you should see the name of the file and a message in the screen.

Figure 236 File Sharing: File Upload



Upload succeeded

Type	File Name	Size	Modified Date	Action
	Standard_SC.ps	491 kb	Thu Dec 7 15:03:18 2006	
	PrintingProcess.doc	31 kb	Thu Dec 7 14:55:00 2006	
	NewBusRoute.pdf	489 kb	Thu Dec 7 14:55:24 2006	
	New Folder	0 kb	Thu Dec 7 15:04:58 2006	
	LogoTest.jpg	5 kb	Thu Dec 7 17:14:54 2006	
	File.RTF	88 kb	Thu Dec 7 17:03:36 2006	
	FeedbackEdit.doc	23 kb	Thu Dec 7 14:55:12 2006	
	2006calender.xls	35 kb	Thu Dec 7 14:55:42 2006	

Uploading a file with the same name and file extension replaces the existing file on the file server. No warning message is displayed.

25

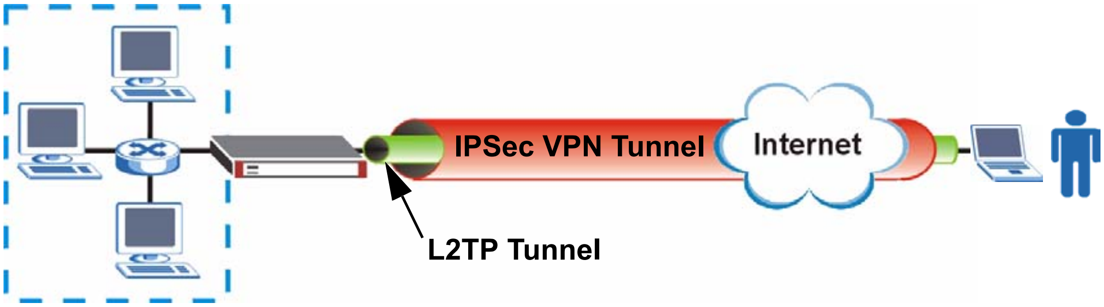
L2TP VPN

This chapter explains how to set up and maintain L2TP VPNs in the ZyWALL. See Section 5.4.6 on page 116 for related information on these screens.

25.1 L2TP VPN Overview

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the ZyWALL. The remote users do not need their own IPSec gateways or VPN client software.

Figure 237 L2TP VPN Overview



The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first (see Chapter 20 on page 291 for information on IPSec) and then an L2TP tunnel is built inside it.

At the time of writing the L2TP remote user must have a public IP address in order for L2TP VPN to work (the remote user cannot be behind a NAT router or a firewall).

25.2 IPSec Configuration

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 20 on page 291 for details). The IPSec VPN connection must:

- Be enabled.

- Use transport mode.
- Not be a manual key VPN connection.
- Use **Pre-Shared Key** authentication.
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

25.2.1 Using the Default L2TP VPN Connection

Default_L2TP_VPN_Connection is pre-configured to be convenient to use for L2TP VPN. If you use it, edit the following.

Configure the local and remote policies as follows.

- For the **Local Policy**, create an address object that uses host type and contains the **My Address** IP address that you configured in the **Default_L2TP_VPN_GW**. Use this address object in the local policy.
- For the **Remote Policy**, create an address object that uses host type and an IP address of 0.0.0.0. Use this address object in the remote policy.

You must also edit the **Default_L2TP_VPN_GW** gateway entry.

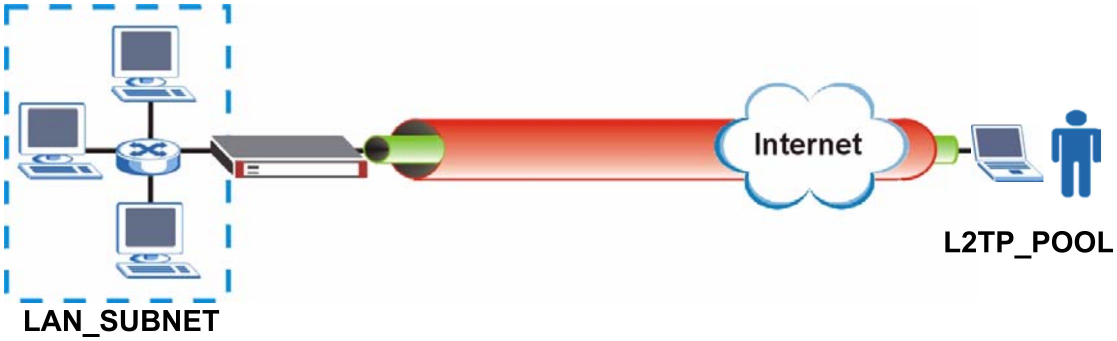
- Configure the **My Address** setting according to your requirements.
- Replace the default **Pre-Shared Key**.

25.3 Policy Route

You must configure a policy route to let remote users access resources on a network behind the ZyWALL.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in the following figure).
- Set the **Destination Address** to the IP address pool that the ZyWALL assigns to the remote users (**L2TP_POOL** in the following figure).
- Set the next hop to be the VPN tunnel that you are using for L2TP.

Figure 238 Policy Route for L2TP VPN

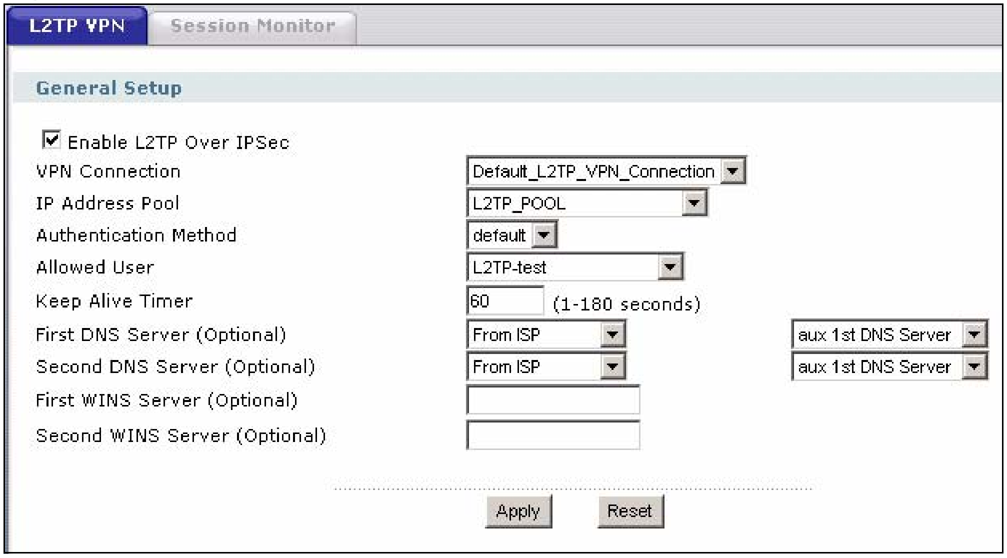


25.4 L2TP VPN Configuration

Click **VPN** > **L2TP VPN** to open the following screen. Use this screen to configure the ZyWALL's L2TP VPN settings.

Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Figure 239 VPN > L2TP VPN



☑ Enable L2TP Over IPSec
VPN Connection: Default_L2TP_VPN_Connection
IP Address Pool: L2TP_POOL
Authentication Method: default
Allowed User: L2TP-test
Keep Alive Timer: 60 (1-180 seconds)
First DNS Server (Optional): From ISP, aux 1st DNS Server
Second DNS Server (Optional): From ISP, aux 1st DNS Server
First WINS Server (Optional):
Second WINS Server (Optional):

The following table describes the fields in this screen.

Table 106 VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
Enable L2TP Over IPSec	Use this field to turn the ZyWALL's L2TP VPN function on or off.
VPN Connection	Select the IPSec VPN connection the ZyWALL uses for L2TP VPN. All of the configured VPN connections display here, but the one you use must meet the requirements listed in Section 25.2 on page 345. Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
IP Address Pool	Select the pool of IP addresses that the ZyWALL uses to assign to the L2TP VPN clients. Select **Create Object** to configure a new pool of IP addresses.
Authentication Method	Select how the ZyWALL authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the ZyWALL check a user's user name and password against the ZyWALL's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these. See Chapter 39 on page 541 for how to create authentication method objects.

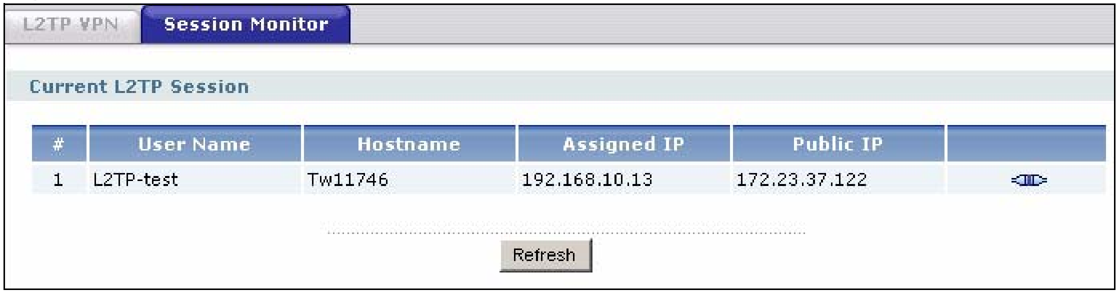
Table 106 VPN > IPSec VPN > VPN Connection (continued)

LABEL	DESCRIPTION
Allowed User	The remote user must log into the ZyWALL to use the L2TP VPN tunnel. Select a user or user group that can use the L2TP VPN tunnel. Select **Create Object** to configure a new user account (see Section 34.2.1 on page 506 for details). Otherwise, select **any** to allow any user with a valid account and password on the ZyWALL to log in.
Keep Alive Timer	The ZyWALL sends a Hello message after waiting this long without receiving any traffic from the remote user. The ZyWALL disconnects the VPN tunnel if the remote user does not respond.
First DNS Server Second DNS Server	Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways. **Custom Defined** - enter a static IP address. **From ISP** - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways.
Apply	Click **Apply** to save your changes in the ZyWALL.
Reset	Click **Cancel** to start configuring this screen afresh.

25.5 L2TP VPN Session Monitor

Click **VPN > L2TP VPN > Session Monitor** to open the following screen. Use this screen to display and manage the ZyWALL's connected L2TP VPN sessions.

Figure 240 VPN > L2TP VPN > Session Monitor



#	User Name	Hostname	Assigned IP	Public IP	
1	L2TP-test	Tw11746	192.168.10.13	172.23.37.122	

The following table describes the fields in this screen.

Table 107 VPN > L2TP VPN > Session Monitor

LABEL	DESCRIPTION
#	This is the index number of a current L2TP VPN session.
User Name	This field displays the remote user's user name.
Hostname	This field displays the name of the computer that has this L2TP VPN connection with the ZyWALL.
Assigned IP	This field displays the IP address that the ZyWALL assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This field displays the public IP address that the remote user is using to connect to the Internet.

Table 107 VPN > L2TP VPN > Session Monitor (continued)

LABEL	DESCRIPTION
Disconnect	Click the **Disconnect** icon next to an L2TP VPN connection to disconnect it.
Refresh	Click **Refresh** to update the information in the display.

26

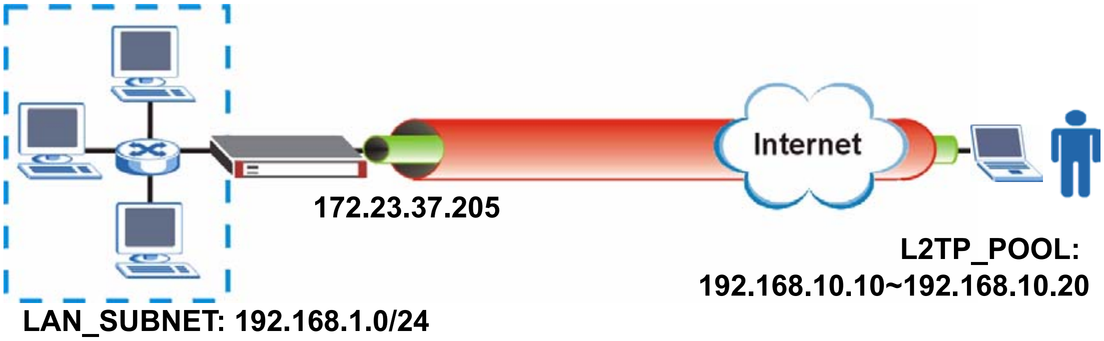
L2TP VPN Example

This chapter shows how to create a basic L2TP VPN tunnel.

26.1 L2TP VPN Example

This chapter uses the following settings in creating a basic L2TP VPN tunnel.

Figure 241 L2TP VPN Example

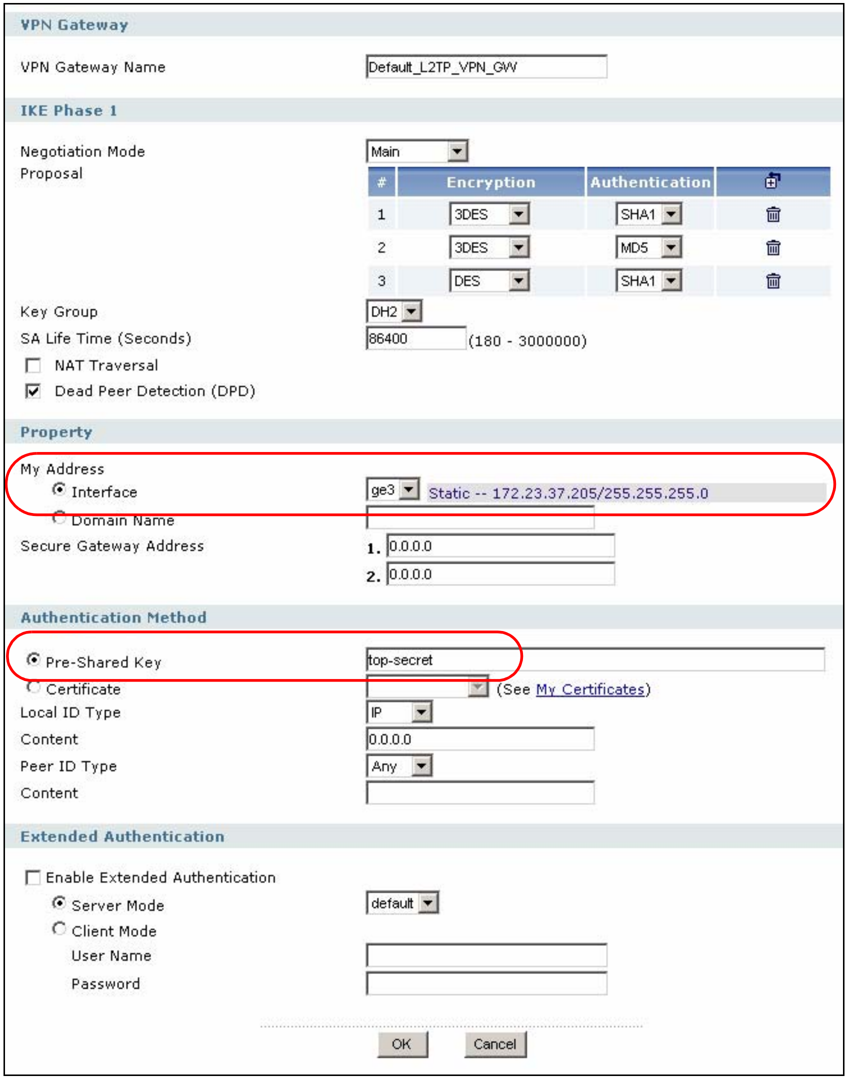


- The ZyWALL has a static IP address of 172.23.37.205 for the ge3 interface.
- The remote user has a dynamic public IP address and connects through the Internet.
- You configure an IP address pool object named **L2TP_POOL** to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the **LAN_SUBNET** which covers the 192.168.1.0/24 subnet.

26.2 Configuring the Default L2TP VPN Gateway Example

1 Click **VPN** > **Network** > **IPSec VPN** > **VPN Gateway** to open the screen that lists the VPN gateways. Click the **Default_L2TP_VPN_GW** entry's **Edit** icon.

Figure 242 VPN > IPSec VPN > VPN Gateway > Edit



VPN Gateway

VPN Gateway Name: Default_L2TP_VPN_GW

IKE Phase 1

Negotiation Mode: Main

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	3DES	MD5
3	DES	SHA1

Key Group: DH2

SA Life Time (Seconds): 86400 (180 - 3000000)

☐ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address

● Interface: ge3 Static -- 172.23.37.205/255.255.255.0

○ Domain Name

Secure Gateway Address: 1. 0.0.0.0 2. 0.0.0.0

Authentication Method

● Pre-Shared Key: top-secret

○ Certificate (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content

Extended Authentication

☐ Enable Extended Authentication

● Server Mode: default

○ Client Mode

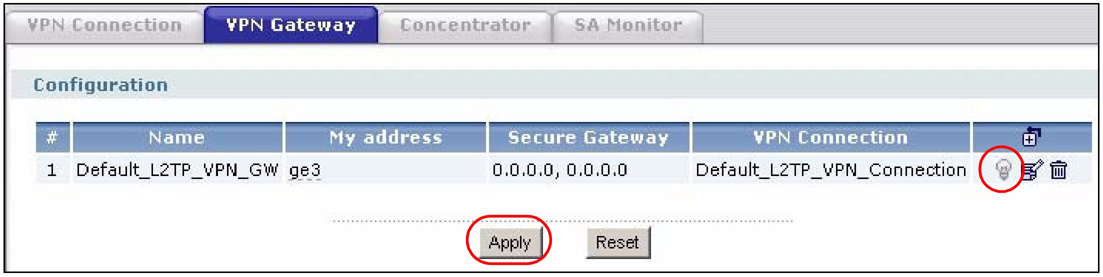
User Name

Password

- Configure the **My Address** setting. This example uses interface ge3 with static IP address 172.23.37.205.
- Configure the **Pre-Shared Key**. This example uses **top-secret**. Click **OK**.

2 Click the **Default_L2TP_VPN_GW** entry's **Enable** icon and click **Apply** to turn on the entry.

Figure 243 VPN > IPSec VPN > VPN Gateway (Enable)



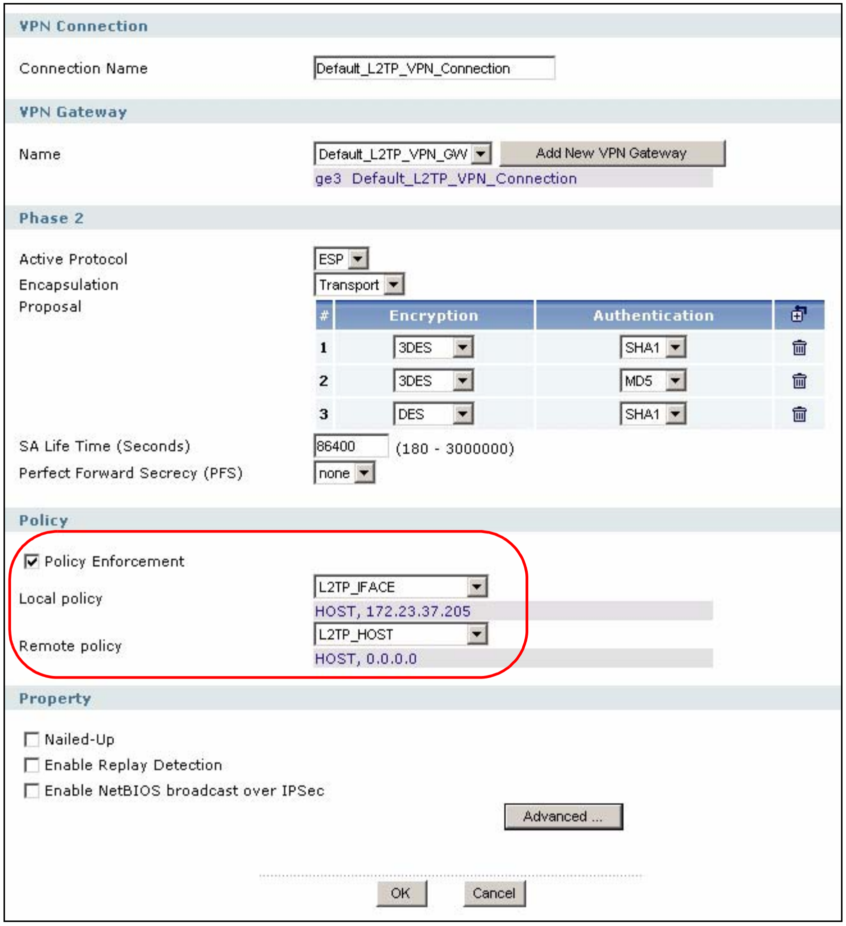
Configuration

#	Name	My address	Secure Gateway	VPN Connection
1	Default_L2TP_VPN_GW	ge3	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection

26.3 Configuring the Default L2TP VPN Connection Example

1 Click **VPN** > **Network** > **IPSec VPN** to open the screen that lists the VPN connections. Click the **Default_L2TP_VPN_Connection**'s **Edit** icon.

Figure 244 VPN > IPSec VPN > VPN Connection > Edit



VPN Connection

Connection Name: Default_L2TP_VPN_Connection

VPN Gateway

Name: Default_L2TP_VPN_GW

ge3 Default_L2TP_VPN_Connection

Phase 2

Active Protocol: ESP

Encapsulation: Transport

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	3DES	MD5
3	DES	SHA1

SA Life Time (Seconds): 86400 (180 - 3000000)

Perfect Forward Secrecy (PFS): none

Policy

☑ Policy Enforcement

Local policy: L2TP_IFACE

HOST, 172.23.37.205

Remote policy: L2TP_HOST

HOST, 0.0.0.0

Property

☐ Nailed-Up

☐ Enable Replay Detection

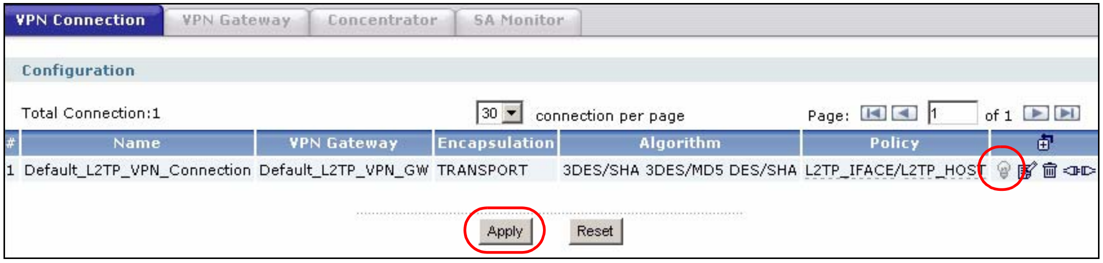
☐ Enable NetBIOS broadcast over IPSec

2 Enforce and configure the local and remote policies.

- For the **Local Policy**, create an address object that uses host type and contains the **My Address** IP address that you configured in the **Default_L2TP_VPN_GW**. The address object in this example uses IP address 172.23.37.205 and is named **L2TP_IFACE**.
- For the **Remote Policy**, create an address object that uses host type and an IP address of 0.0.0.0. It is named **L2TP_HOST** in this example.

3 Click the **Default_L2TP_VPN_Connection** entry's **Enable** icon and click **Apply** to turn on the entry.

Figure 245 VPN > IPSec VPN > VPN Connection (Enable)



Total Connection:1

30 connection per page

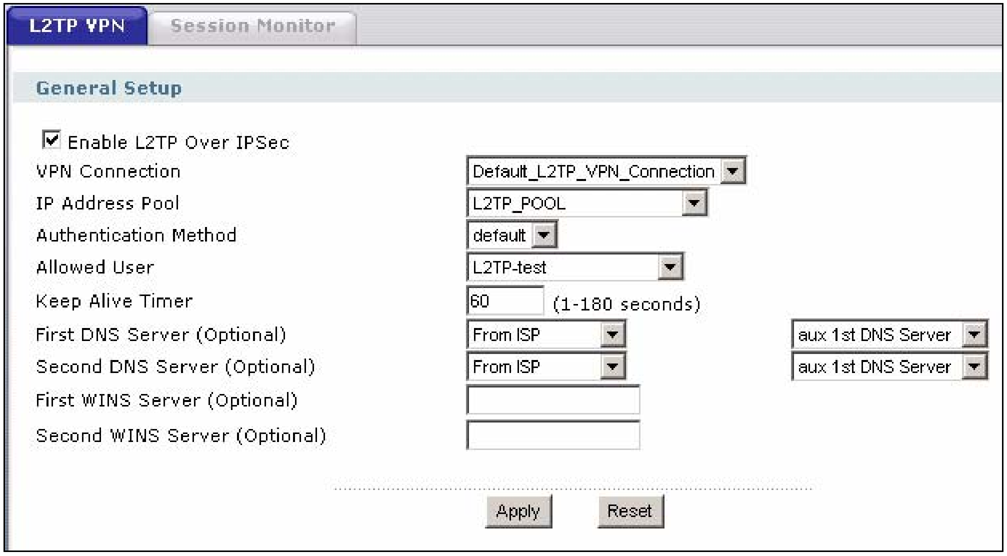
Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TRANSPORT	3DES/SHA 3DES/MD5 DES/SHA	L2TP_IFACE/L2TP_HOST

26.4 Configuring the L2TP VPN Settings Example

1 Click **VPN** > **L2TP VPN** to open the following screen.

Figure 246 VPN > L2TP VPN Example



☑ Enable L2TP Over IPSec

VPN Connection	Default_L2TP_VPN_Connection	
IP Address Pool	L2TP_POOL	
Authentication Method	default	
Allowed User	L2TP-test	
Keep Alive Timer	60 (1-180 seconds)	
First DNS Server (Optional)	From ISP	aux 1st DNS Server
Second DNS Server (Optional)	From ISP	aux 1st DNS Server
First WINS Server (Optional)		
Second WINS Server (Optional)		

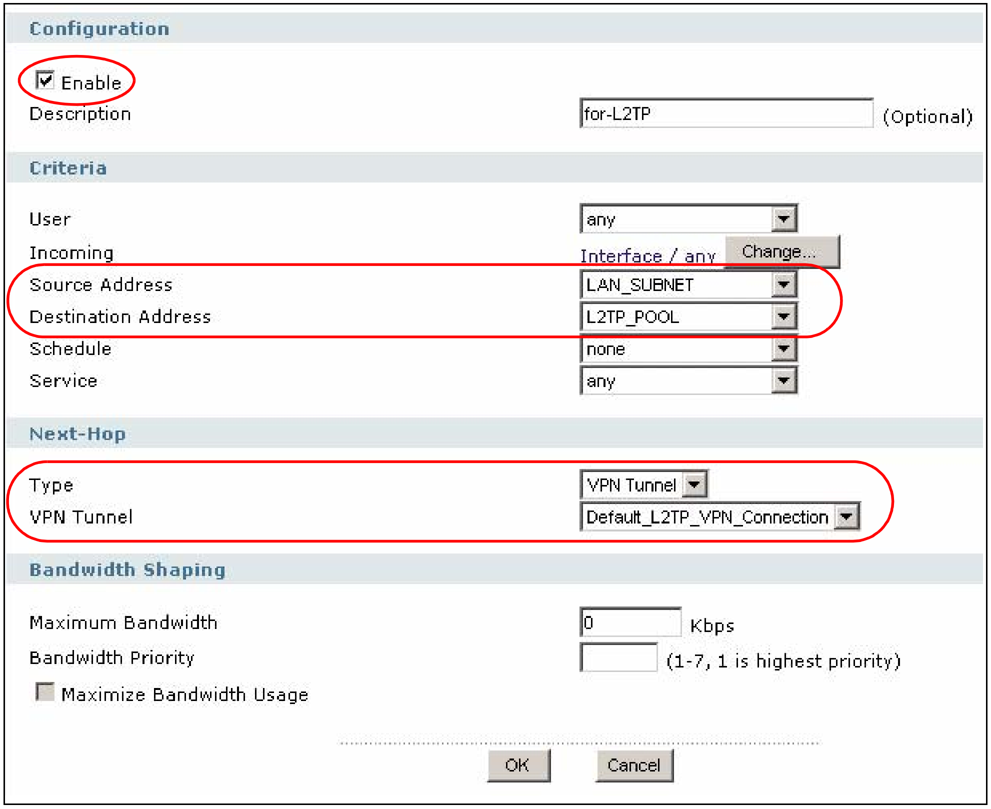
2 Configure the following.

- Enable the connection.
- Set it to use the **Default_L2TP_VPN_Connection** VPN connection.
- Configure an IP address pool for the range of 192.168.10.10 to 192.168.10.20. It is called **L2TP_POOL** here.
- This example uses the default authentication method (the ZyWALL’s local user data base).
- Select a user or group of users that can use the tunnel. Here a user account named **L2TP-test** has been created.
- The other fields are left to the defaults in this example, click **Apply**.

26.5 Configuring the Policy Route for L2TP Example

1 Click **Routing** > **Add** to open the following screen.

Figure 247 Routing > Add: L2TP VPN Example



Configuration

☑ Enable

Description: for-L2TP (Optional)

Criteria

User: any

Incoming: Interface / any

Source Address: LAN_SUBNET

Destination Address: L2TP_POOL

Schedule: none

Service: any

Next-Hop

Type: VPN Tunnel

VPN Tunnel: Default_L2TP_VPN_Connection

Bandwidth Shaping

Maximum Bandwidth: 0 Kbps

Bandwidth Priority: (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

2 Configure the following.

- Enable the policy route.
- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in this example).
- Set the **Destination Address** to the IP address pool that the ZyWALL assigns to the remote users (**L2TP_POOL** in this example).
- Set the next hop to be the **Default_L2TP_VPN_Connection** VPN tunnel.
- Click **OK**.

26.6 Configuring L2TP VPN in Windows XP and 2000

The following sections cover how to configure L2TP in remote user computers using Windows XP and Windows 2000. The example settings in these sections go along with the L2TP VPN configuration example in Section 26.1 on page 351.

Before you configure the client, issue one of the following commands from the Windows command prompt to make sure the computer is running the Microsoft IPSec service. Make sure you include the quotes.

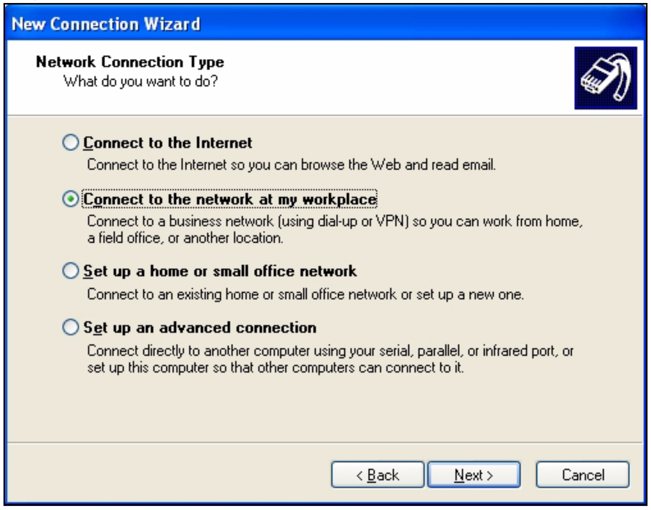
- For Windows XP. use `net start "ipsec services"`.
- For Windows 2000, use `net start "ipsec policy agent"`.

26.6.1 Configuring L2TP in Windows XP

In Windows XP do the following to establish an L2TP VPN connection.

1. Click **Start** > **Control Panel** > **Network Connections** > **New Connection Wizard**.
2. Click **Next** in the **Welcome** screen.
3. Select **Connect to the network at my workplace** and click **Next**.

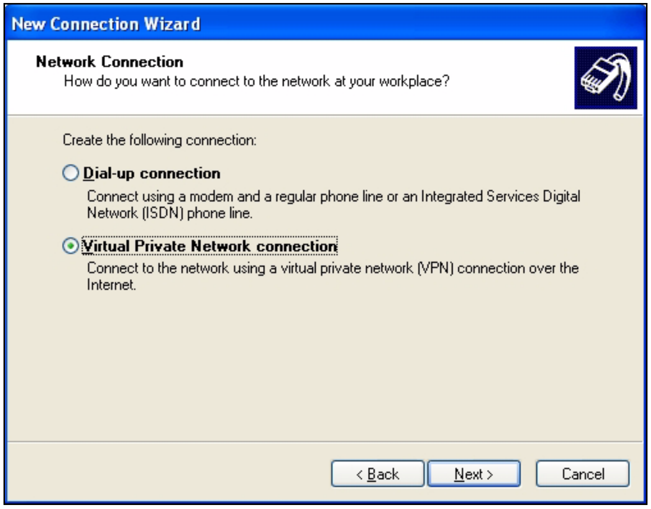
Figure 248 New Connection Wizard: Network Connection Type



New Connection Wizard
Network Connection Type
What do you want to do?
○ Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
● Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
○ Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
○ Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

4. Select **Virtual Private Network connection** and click **Next**.

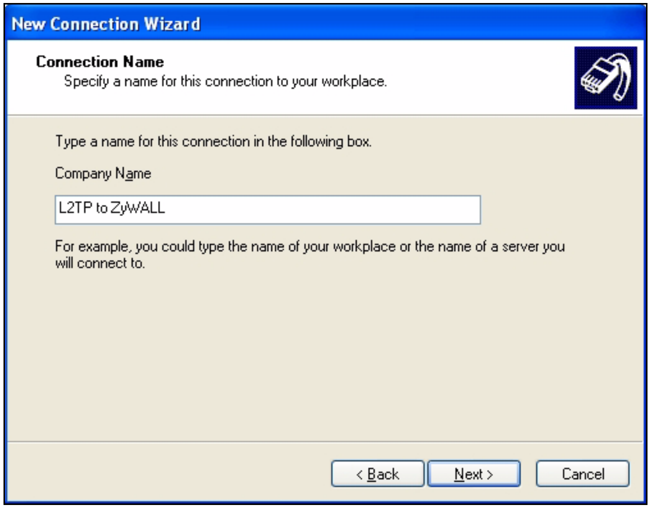
Figure 249 New Connection Wizard: Network Connection



New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
○ Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
● Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

5. Type **L2TP to ZyWALL** as the **Company Name**.

Figure 250 New Connection Wizard: Connection Name



Connection Name

Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

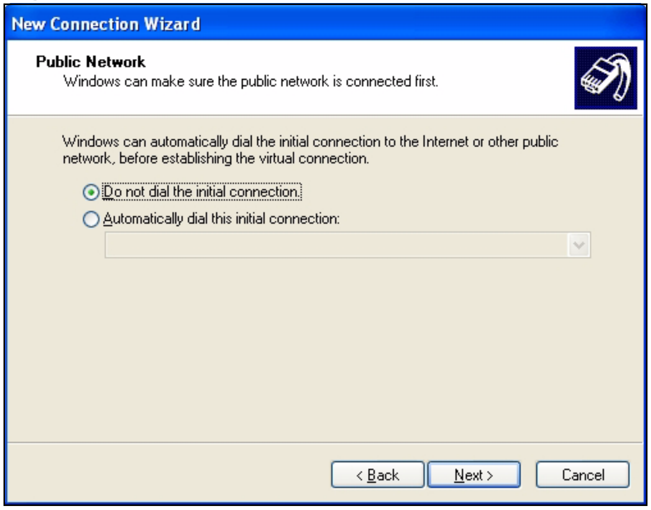
Company Name

L2TP to ZyWALL

For example, you could type the name of your workplace or the name of a server you will connect to.

6 Select **Do not dial the initial connection** and click **Next**.

Figure 251 New Connection Wizard: Public Network



Public Network

Windows can make sure the public network is connected first.

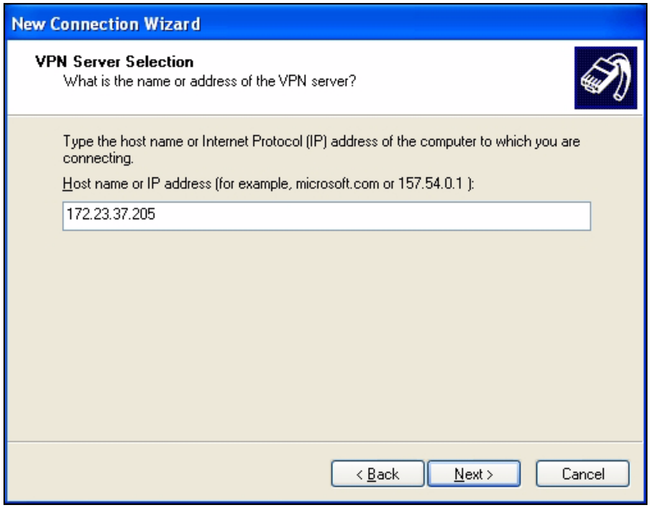
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

● Do not dial the initial connection.

○ Automatically dial this initial connection:

7 Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the ZyWALL is using for L2TP VPN (172.23.37.205 in this example).

Figure 252 New Connection Wizard: VPN Server Selection



New Connection Wizard

VPN Server Selection

What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

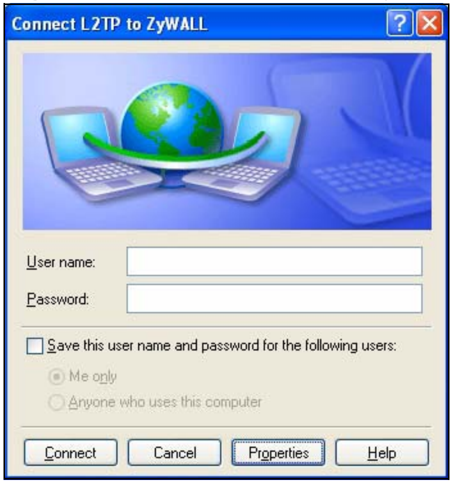
Host name or IP address (for example, microsoft.com or 157.54.0.1):

172.23.37.205

8 Click **Finish**.

9 The **Connect L2TP to ZyWALL** screen appears. Click **Properties** > **Security**.

Figure 253 Connect L2TP to ZyWALL



Connect L2TP to ZyWALL

User name:

Password:

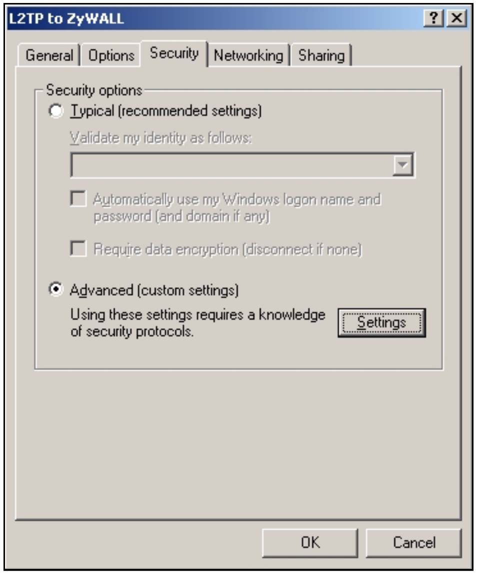
☐ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

10 Click **Security**, select **Advanced (custom settings)** and click **Settings**.

Figure 254 Connect L2TP to ZyWALL: Security



L2TP to ZyWALL
General
Options
Security
Networking
Sharing
Settings
OK
Cancel

Security options

○ Typical (recommended settings)

Validate my identity as follows:

☐ Automatically use my Windows logon name and password (and domain if any)

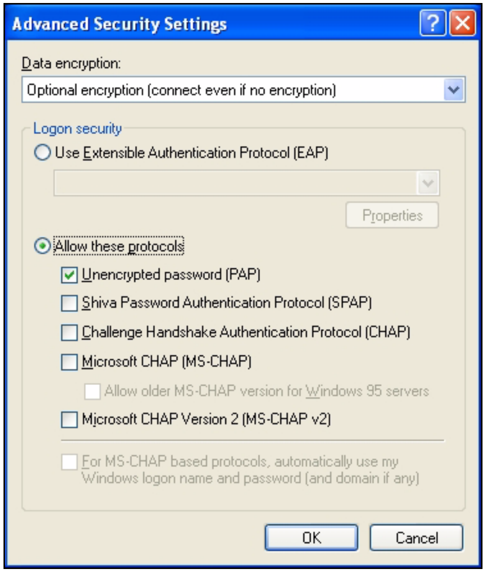
☐ Require data encryption (disconnect if none)

● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

11 Select **Optional encryption (connect even if no encryption)** and the **Allow these protocols** radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**.

Figure 255 Connect ZyWALL L2TP: Security > Advanced



Advanced Security Settings
Properties
OK
Cancel

Data encryption:

Optional encryption (connect even if no encryption)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

☑ Unencrypted password (PAP)

☐ Shiva Password Authentication Protocol (SPAP)

☐ Challenge Handshake Authentication Protocol (CHAP)

☐ Microsoft CHAP (MS-CHAP)

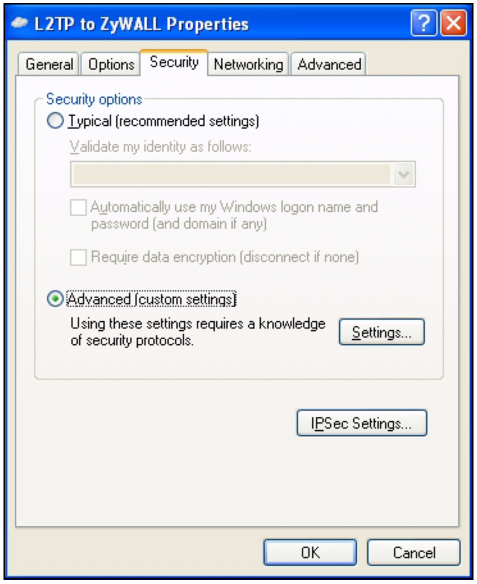
☐ Allow older MS-CHAP version for Windows 95 servers

☐ Microsoft CHAP Version 2 (MS-CHAP v2)

☐ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

12 Click **IPSec Settings**.

Figure 256 L2TP to ZyWALL Properties > Security



L2TP to ZyWALL Properties

General
Options
Security
Networking
Advanced

Security options

○ Typical (recommended settings)

Validate my identity as follows:

☐ Automatically use my Windows logon name and password (and domain if any)

☐ Require data encryption (disconnect if none)

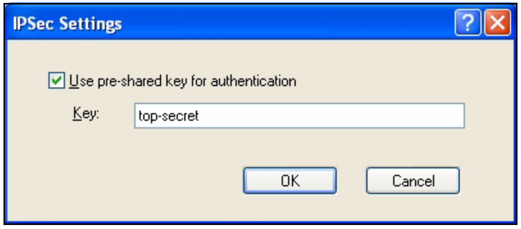
● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

Settings...
IPSec Settings...
OK
Cancel

13 Select the **Use pre-shared key for authentication** check box and enter the pre-shared key used in the VPN gateway configuration that the ZyWALL is using for L2TP VPN. Click **OK**.

Figure 257 L2TP to ZyWALL Properties > Security > IPSec Settings



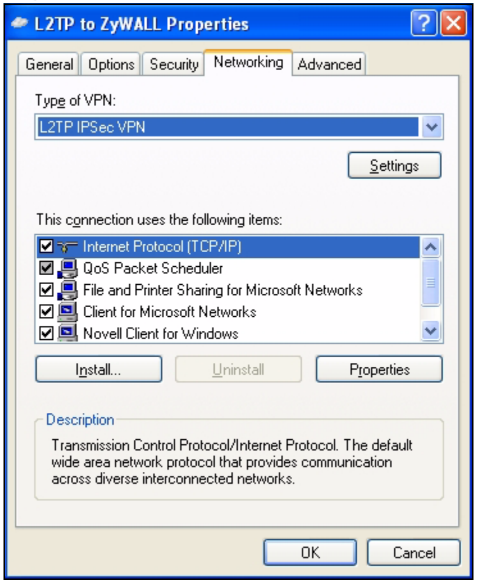
IPSec Settings

☑ Use pre-shared key for authentication

Key: top-secret

14 Click **Networking**. Select **L2TP IPSec VPN** as the **Type of VPN**. Click **OK**.

Figure 258 L2TP to ZyWALL Properties: Networking



L2TP to ZyWALL Properties

General
Options
Security
Networking
Advanced

Type of VPN: L2TP IPSec VPN

This connection uses the following items:

☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks
☑ Novell Client for Windows

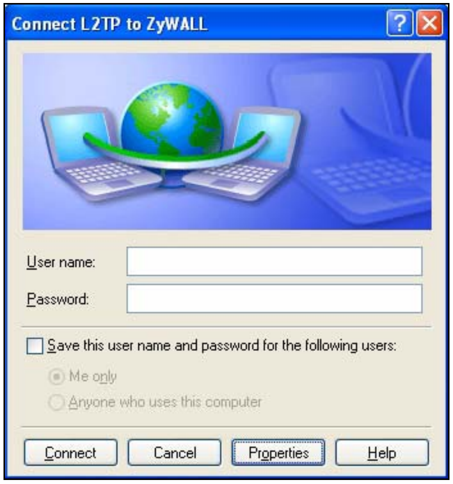
Settings
Install...
Uninstall
Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

15 Enter the user name and password of your ZyWALL account. Click **Connect**.

Figure 259 Connect L2TP to ZyWALL


Connect L2TP to ZyWALL
User name:
Password:
☐ Save this user name and password for the following users:
● Me only
○ Anyone who uses this computer
Connect
Cancel
Properties
Help

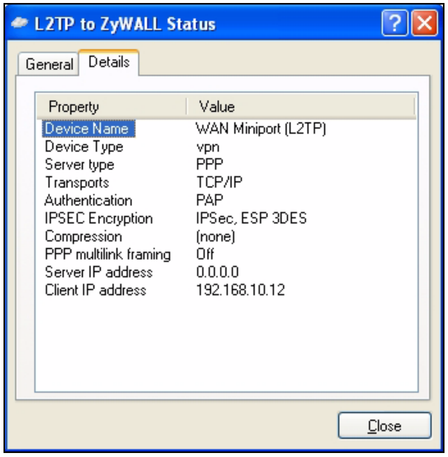
16 A window appears while the user name and password are verified.

17 A ZyWALL-L2TP icon displays in your system tray. Double-click it to open a status screen.

Figure 260 ZyWALL-L2TP System Tray Icon

18 Click **Details** to see the address that you received is from the L2TP range you specified on the ZyWALL (192.168.10.10-192.168.10.20).

Figure 261 ZyWALL-L2TP Status: Details


L2TP to ZyWALL Status
General
Details
Close

Property	Value
Device Name	WAN Miniport (L2TP)
Device Type	vpn
Server type	PPP
Transports	TCP/IP
Authentication	PAP
IPSEC Encryption	IPSec, ESP 3DES
Compression	(none)
PPP multilink framing	Off
Server IP address	0.0.0.0
Client IP address	192.168.10.12

19 Access a server or other network resource behind the ZyWALL to make sure your access works.

26.6.2 Configuring L2TP in Windows 2000

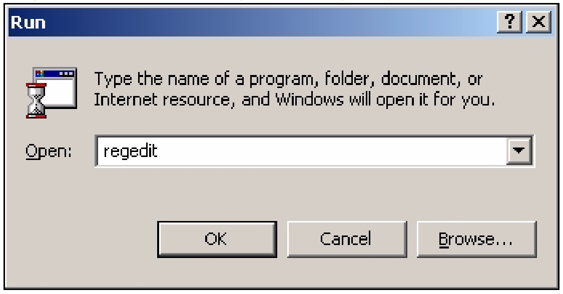
Windows 2000 does not support using pre-shared keys by default. Use the following procedures to edit the registry and then configure the computer to use the L2TP client.

26.6.2.1 Editing the Windows 2000 Registry

In Windows 2000, you need to create a registry entry and restart the computer to have it use pre-shared keys.

1 Click **Start** > **Run**. Type `regedit` and click **OK**.

Figure 262 Starting the Registry Editor


Run
?
×
OK
Cancel
Browse...

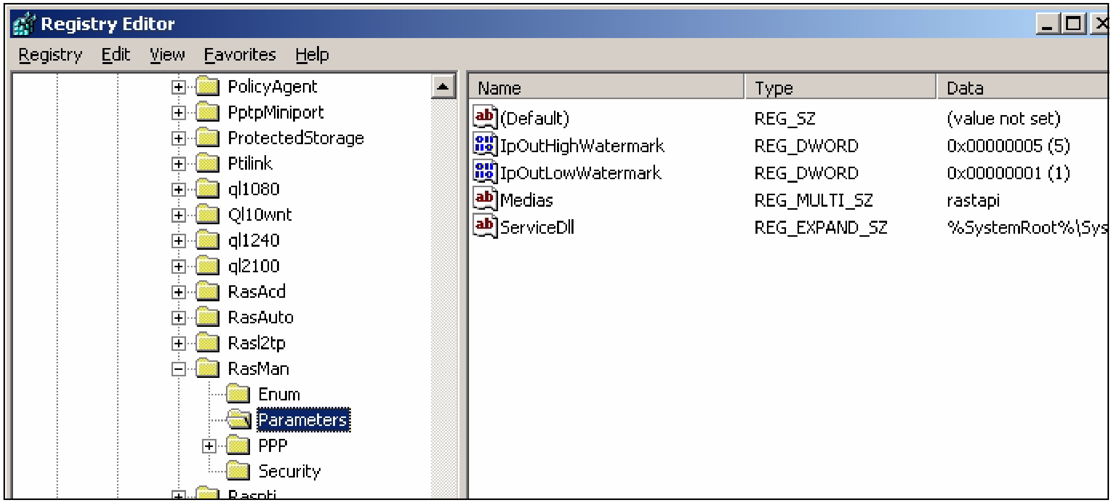
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

2 Click **Registry** > **Export Registry File** and save a backup copy of your registry. You can go back to using this backup if you misconfigure the registry settings.

3 Select **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters**.

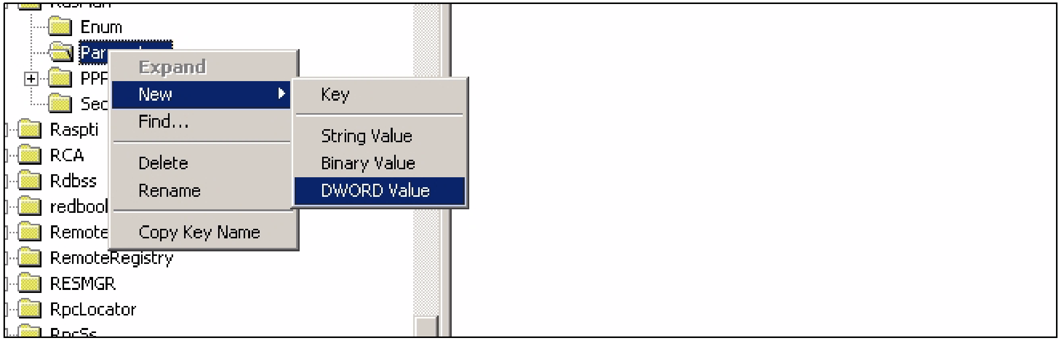
Figure 263 Registry Key


Registry Editor
Registry
Edit
View
Favorites
Help
PolicyAgent
PptpMiniport
ProtectedStorage
Ptilink
ql1080
Ql10wnt
ql1240
ql2100
RasAcd
RasAuto
Rasl2tp
RasMan
Enum
Parameters
PPP
Security
Raspti

Name	Type	Data
(Default)	REG_SZ	(value not set)
IpOutHighWatermark	REG_DWORD	0x00000005 (5)
IpOutLowWatermark	REG_DWORD	0x00000001 (1)
Medias	REG_MULTI_SZ	rastapi
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\Sys

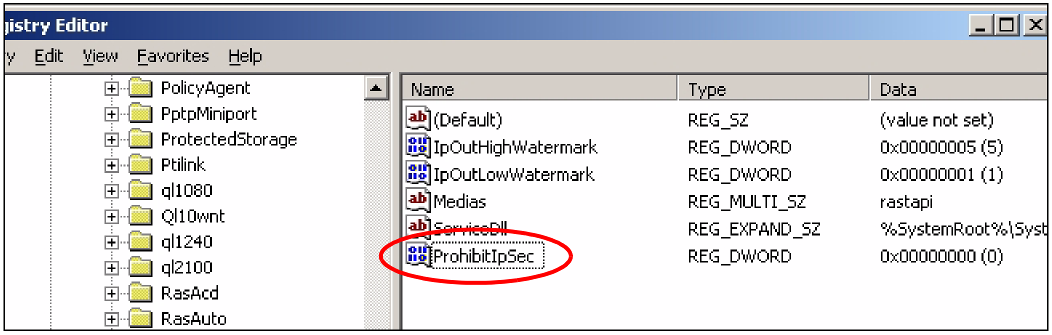
4 Right-click **Parameters** and select **New** > **DWORD Value**.

Figure 264 New DWORD Value


Enum
Par
PPP
Sec
Raspti
RCA
Rdbss
redbool
Remote
RemoteRegistry
RESMGR
RpcLocator
Expand
New
Find...
Delete
Rename
Copy Key Name
Key
String Value
Binary Value
DWORD Value

5 Enter **ProhibitIpSec** as the name. And make sure the **Data** displays as 0’s.

Figure 265 ProhibitIpSec DWORD Value


jistry Editor
y Edit View Favorites Help
PolicyAgent
PptpMiniport
ProtectedStorage
Ptilink
ql1080
Ql10wnt
ql1240
ql2100
RasAcd
RasAuto

Name	Type	Data
(Default)	REG_SZ	(value not set)
IpOutHighWatermark	REG_DWORD	0x00000005 (5)
IpOutLowWatermark	REG_DWORD	0x00000001 (1)
Medias	REG_MULTI_SZ	rastapi
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\Syst
ProhibitIpSec	REG_DWORD	0x00000000 (0)

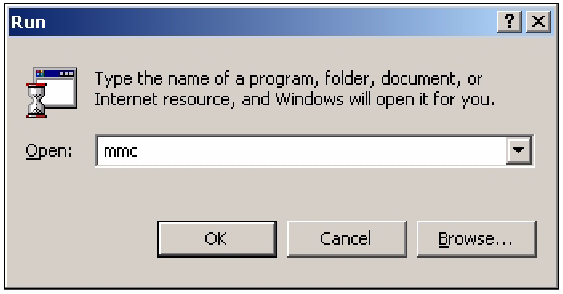
6 Restart the computer and continue with the next section.

26.6.2.2 Configure the Windows 2000 IPSec Policy

After you have created the registry entry and restarted the computer, use these directions to configure an IPSec policy for the computer to use.

1 Click **Start** > **Run**. Type `mmc` and click **OK**.

Figure 266 Run mmc


Run

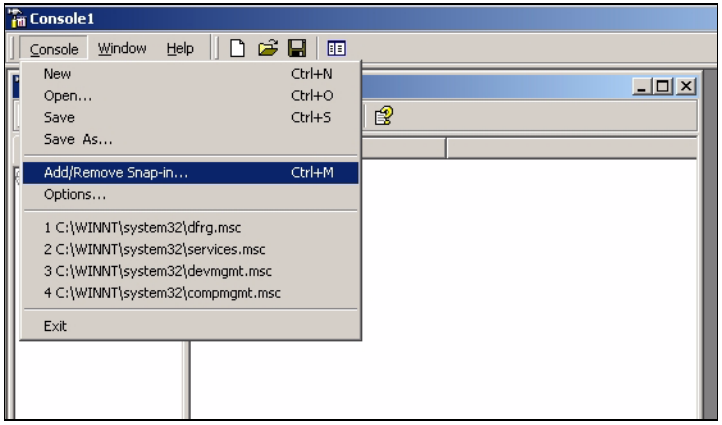
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

OK
Cancel
Browse...

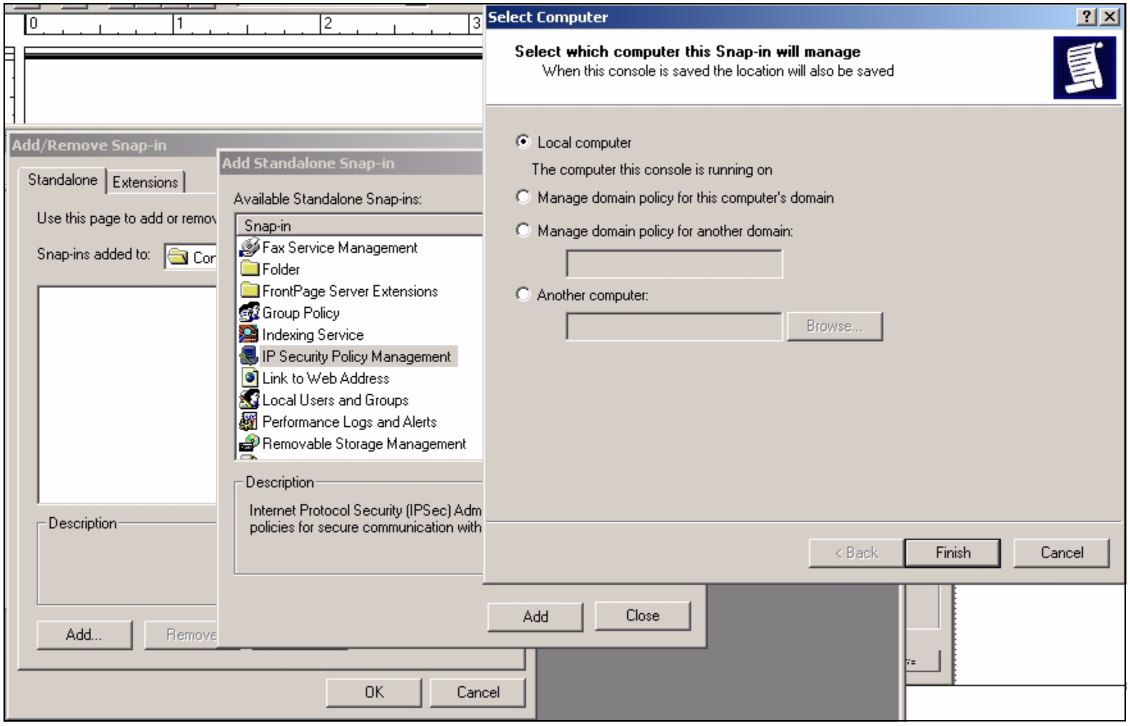
2 Click **Console** > **Add/Remove Snap-in**.

Figure 267 Console > Add/Remove Snap-in


Console1
Console Window Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\WINNT\system32\dfrg.msc
2 C:\WINNT\system32\services.msc
3 C:\WINNT\system32\devmgmt.msc
4 C:\WINNT\system32\compmgmt.msc
Exit

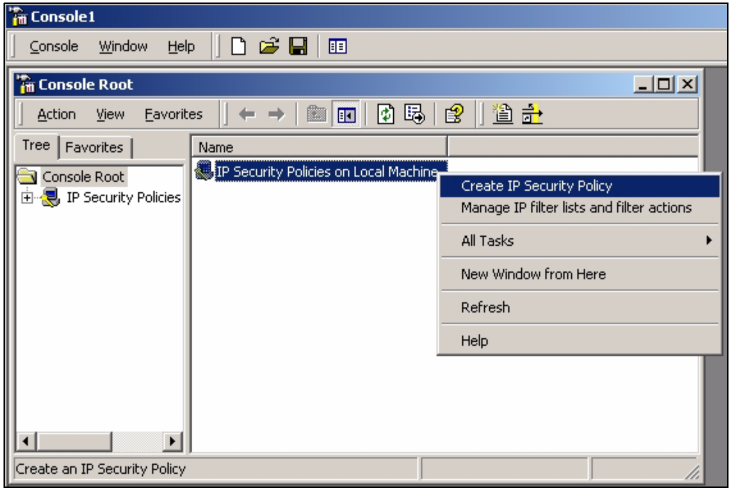
3 Click **Add** > **IP Security Policy Management** >**Add** > **Finish**. Click **Close** > **OK**.

Figure 268 Add > IP Security Policy Management > Finish


Add/Remove Snap-in
Standalone
Extensions
Use this page to add or remov
Snap-ins added to:
Cor
Description
Add...
Remove
OK
Cancel
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in
Fax Service Management
Folder
FrontPage Server Extensions
Group Policy
Indexing Service
IP Security Policy Management
Link to Web Address
Local Users and Groups
Performance Logs and Alerts
Removable Storage Management
Description
Internet Protocol Security (IPSec) Adm
policies for secure communication with
Add
Close
Select Computer
Select which computer this Snap-in will manage
When this console is saved the location will also be saved
● Local computer
The computer this console is running on
○ Manage domain policy for this computer's domain
○ Manage domain policy for another domain:
○ Another computer:
Browse...
< Back
Finish
Cancel

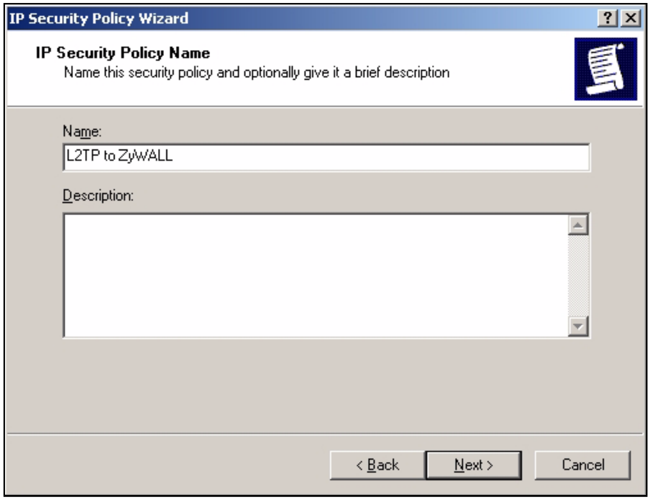
4 Right-click **IP Security Policies on Local Machine** and click **Create IP Security Policy**. Click **Next** in the welcome screen.

Figure 269 Create IP Security Policy


Console1
Console
Window
Help
Console Root
Action
View
Favorites
Tree
Favorites
Console Root
IP Security Policies
Name
IP Security Policies on Local Machine
Create IP Security Policy
Manage IP filter lists and filter actions
All Tasks
New Window from Here
Refresh
Help
Create an IP Security Policy

5 Name the IP security policy **L2TP to ZyWALL**, and click **Next**.

Figure 270 IP Security Policy: Name


IP Security Policy Wizard

IP Security Policy Name

Name this security policy and optionally give it a brief description

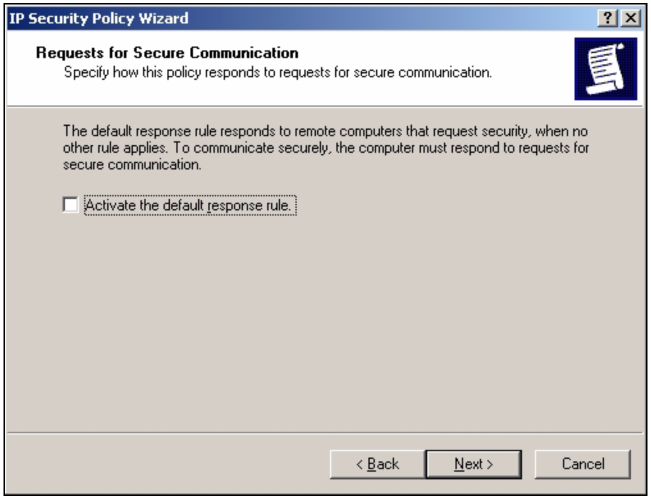
Name: L2TP to ZyWALL

Description:

< Back
Next >
Cancel

6 Clear the **Activate the default response rule** check box and click **Next**.

Figure 271 IP Security Policy: Request for Secure Communication


IP Security Policy Wizard

Requests for Secure Communication

Specify how this policy responds to requests for secure communication.

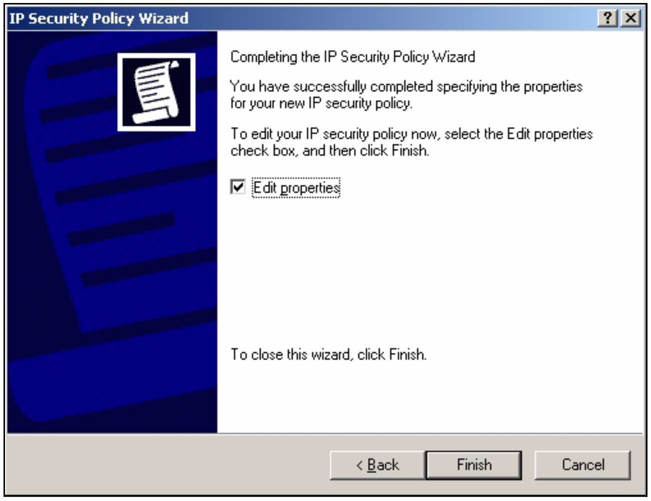
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

☐ Activate the default response rule.

< Back
Next >
Cancel

7 Leave the **Edit Properties** check box selected and click **Finish**.

Figure 272 IP Security Policy: Completing the IP Security Policy Wizard


IP Security Policy Wizard

Completing the IP Security Policy Wizard

You have successfully completed specifying the properties for your new IP security policy.

To edit your IP security policy now, select the Edit properties check box, and then click Finish.

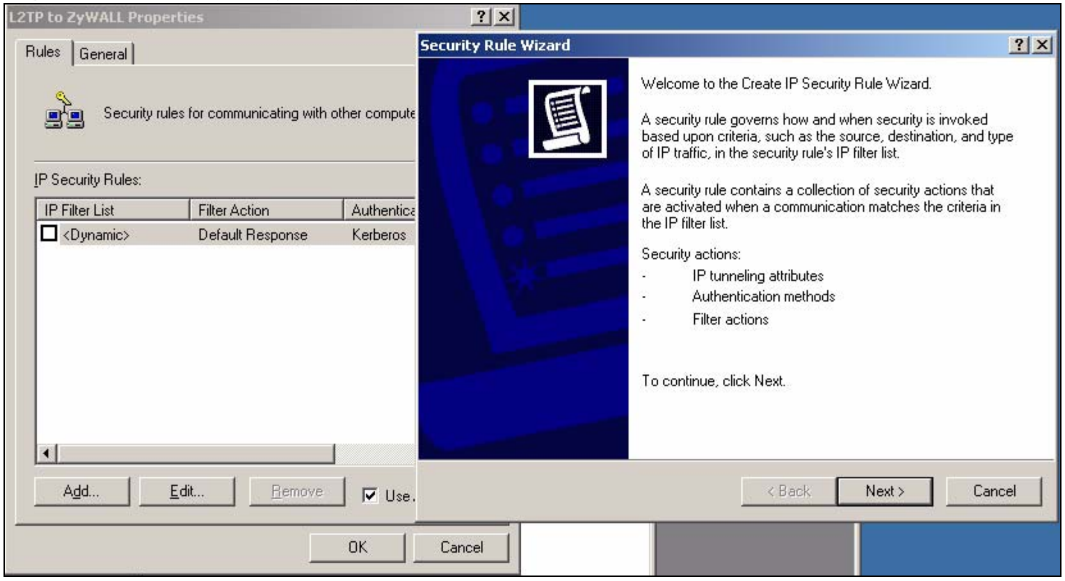
☑ Edit properties

To close this wizard, click Finish.

< Back
Finish
Cancel

8 In the properties dialog box, click **Add** > **Next**.

Figure 273 IP Security Policy Properties > Add


L2TP to ZyWALL Properties
Rules
General
Security rules for communicating with other compute
IP Security Rules:
IP Filter List
Filter Action
Authentica
<Dynamic>
Default Response
Kerberos
Add...
Edit...
Remove
Use
OK
Cancel
Security Rule Wizard
< Back
Next >
Cancel

Welcome to the Create IP Security Rule Wizard.

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

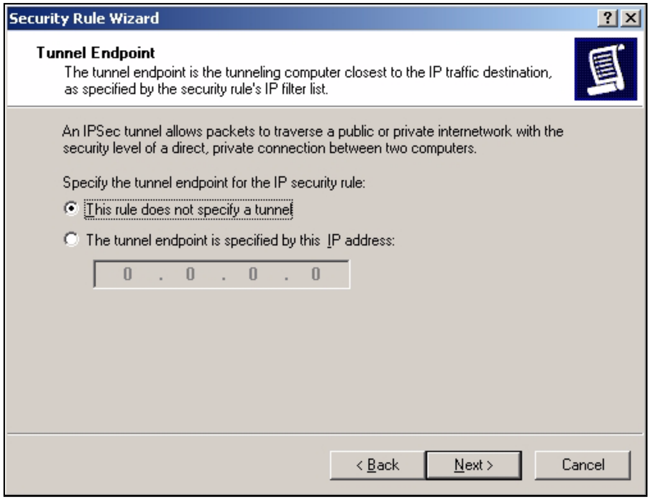
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:
- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

9 Select **This rule does not specify a tunnel** and click **Next**.

Figure 274 IP Security Policy Properties: Tunnel Endpoint


Security Rule Wizard
Tunnel Endpoint
< Back
Next >
Cancel

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

Specify the tunnel endpoint for the IP security rule:

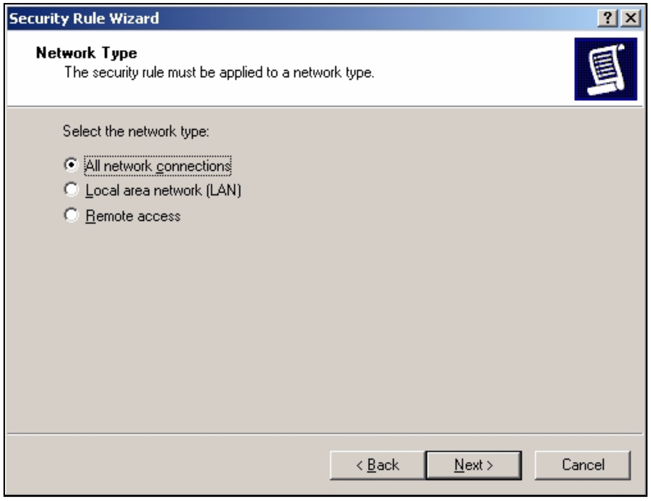
● This rule does not specify a tunnel

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

10 Select **All network connections** and click **Next**.

Figure 275 IP Security Policy Properties: Network Type



Security Rule Wizard

Network Type

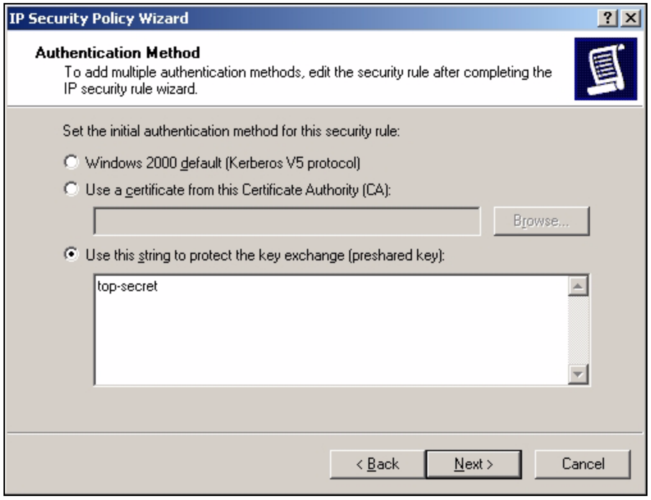
The security rule must be applied to a network type.

Select the network type:

- ● All network connections
- ○ Local area network (LAN)
- ○ Remote access

11 Select **Use this string to protect the key exchange (preshared key)**, type **password** in the text box, and click **Next**.

Figure 276 IP Security Policy Properties: Authentication Method



IP Security Policy Wizard

Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.

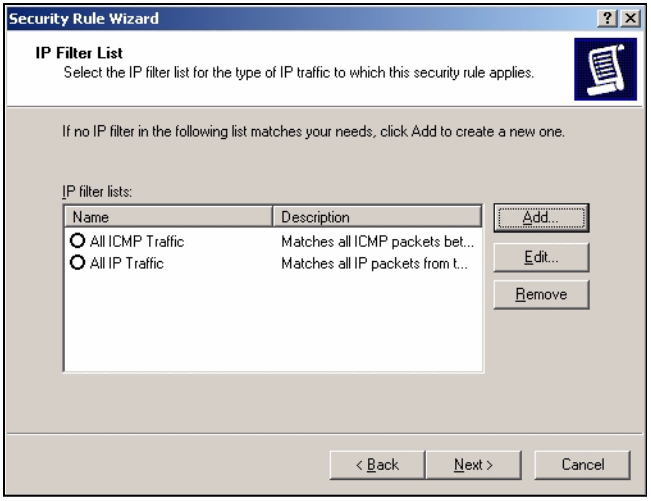
Set the initial authentication method for this security rule:

- ○ Windows 2000 default (Kerberos V5 protocol)
- ○ Use a certificate from this Certificate Authority (CA):
- ● Use this string to protect the key exchange (preshared key):

top-secret

12 Click **Add**.

Figure 277 IP Security Policy Properties: IP Filter List



Security Rule Wizard

IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

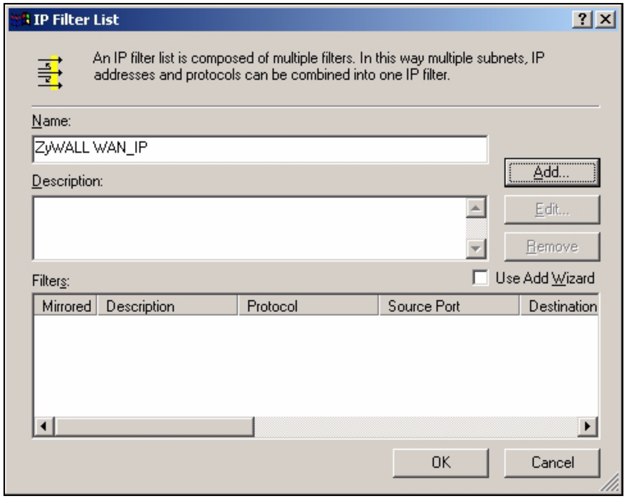
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

13 Type **ZyWALL WAN_IP** in the **Name** field. Clear the **Use Add Wizard** check box and click **Add**.

Figure 278 IP Security Policy Properties: IP Filter List > Add



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: ZyWALL WAN_IP

Description:

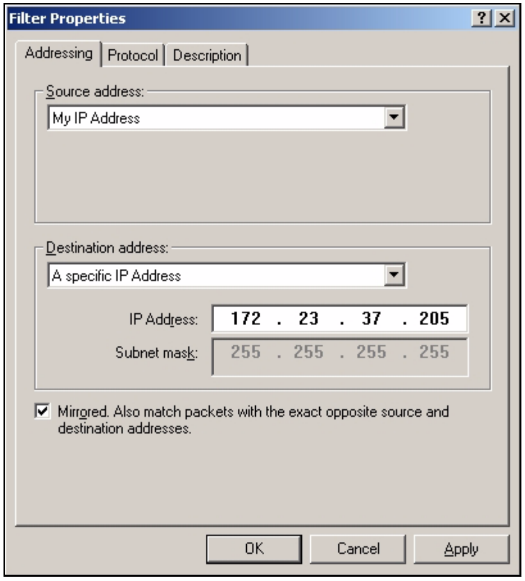
Filters:

☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

14 Configure the following in the **Addressing** tab. Select **My IP Address** in the **Source address** drop-down list box. Select **A specific IP Address** in the **Destination address** drop-down list box and type the ZyWALL's WAN IP address (172.23.37.205 in this example) in the **IP Address** field. Make certain the **Mirrored. Also match packets with the exact opposite source and destination addresses** check box is selected and click **Apply**.

Figure 279 Filter Properties: Addressing


Filter Properties
Addressing
Protocol
Description
OK
Cancel
Apply

Source address: My IP Address

Destination address: A specific IP Address

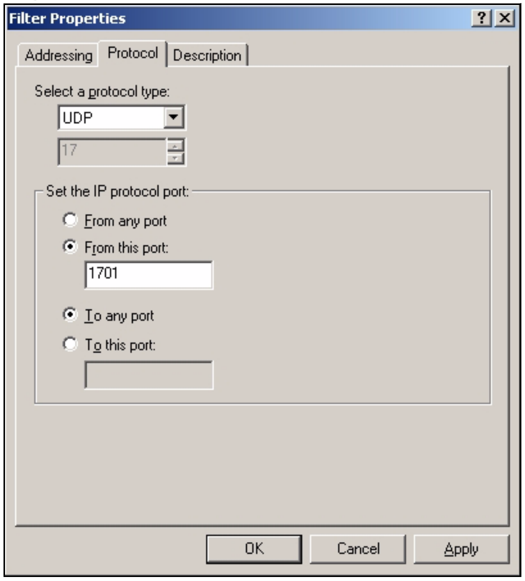
IP Address: 172 . 23 . 37 . 205

Subnet mask: 255 . 255 . 255 . 255

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

15 Configure the following in the **Filter Properties** window's **Protocol** tab. Set the protocol type to **UDP** from port 1701. Select **To any port**. Click **Apply**, **OK,** and then **Close**.

Figure 280 Filter Properties: Protocol


Filter Properties
Addressing
Protocol
Description
OK
Cancel
Apply

Select a protocol type: UDP

17

Set the IP protocol port:

○ From any port

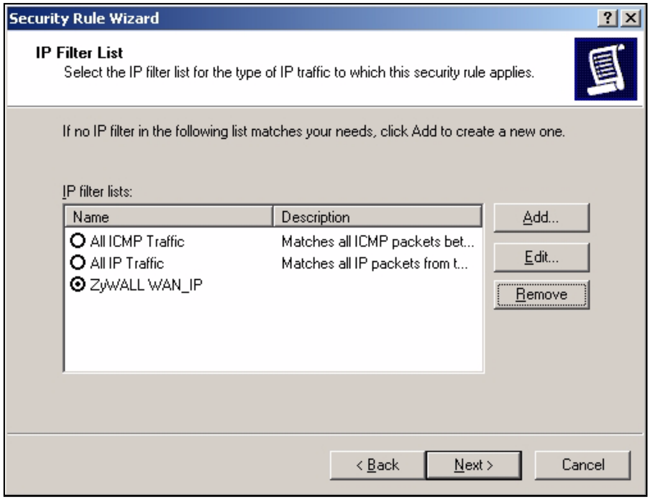
● From this port: 1701

● To any port

○ To this port:

16 Select **ZyWALL WAN_IP** and click **Next**.

Figure 281   IP Security Policy Properties: IP Filter List



Security Rule Wizard

IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

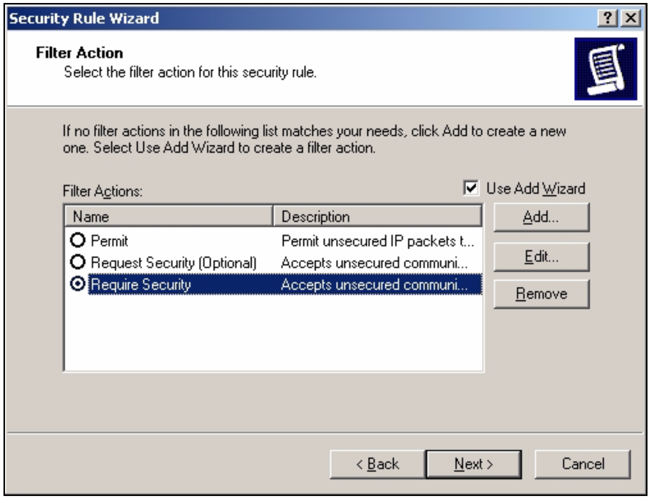
IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
● ZyWALL WAN_IP	

Add...
Edit...
Remove
< Back
Next >
Cancel

17 Select **Require Security** and click **Next**. Then click **Finish** and **Close**.

Figure 282   IP Security Policy Properties: IP Filter List



Security Rule Wizard

Filter Action

Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.

Filter Actions:

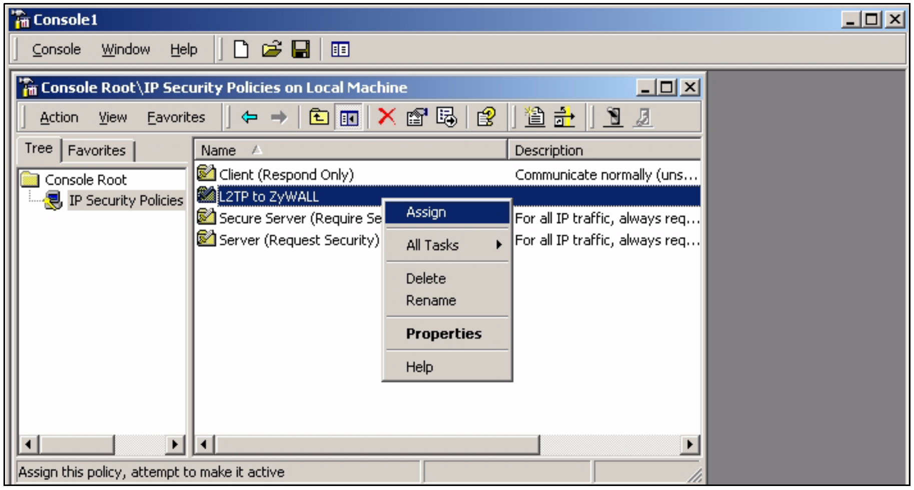
☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
● Require Security	Accepts unsecured communi...

Add...
Edit...
Remove
< Back
Next >
Cancel

18 In the **Console** window, right-click **L2TP to ZyWALL** and select **Assign**.

Figure 283   Console: L2TP to ZyWALL Assign



Console1

Console Root\IP Security Policies on Local Machine

Name	Description
Client (Respond Only)	Communicate normally (uns...
L2TP to ZyWALL	
Secure Server (Require Se	For all IP traffic, always req...
Server (Request Security)	For all IP traffic, always req...

Assign this policy, attempt to make it active

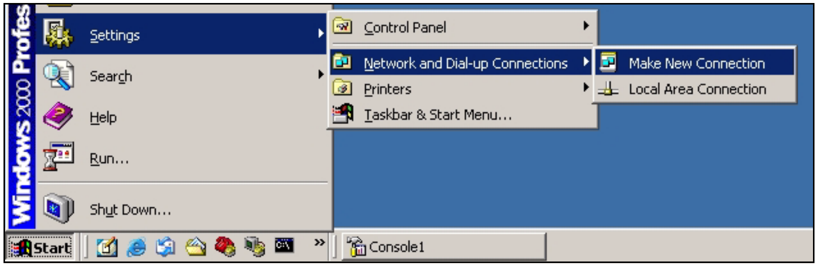
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
IP Security Policies
Assign
All Tasks
Delete
Rename
Properties
Help

26.6.2.3 Configure the Windows 2000 Network Connection

After you have configured the IPSec policy, use these directions to create a network connection.

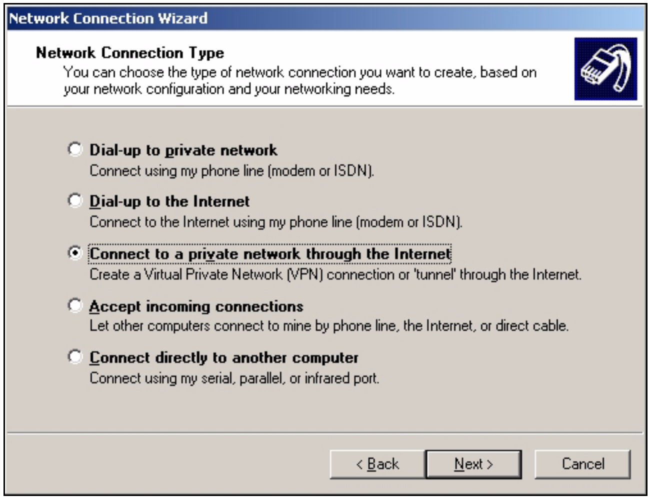
1 Click **Start** > **Settings** > **Network and Dial-up connections** > **Make New Connection**. In the wizard welcome screen, click **Next**.

Figure 284 Start New Connection Wizard


Windows 2000 Profes
Settings
Search
Help
Run...
Shut Down...
Start
Console1
Control Panel
Network and Dial-up Connections
Printers
Taskbar & Start Menu...
Make New Connection
Local Area Connection

2 Select **Connect to a private network through the Internet** and click **Next**.

Figure 285 New Connection Wizard: Network Connection Type


Network Connection Wizard

Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

● **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

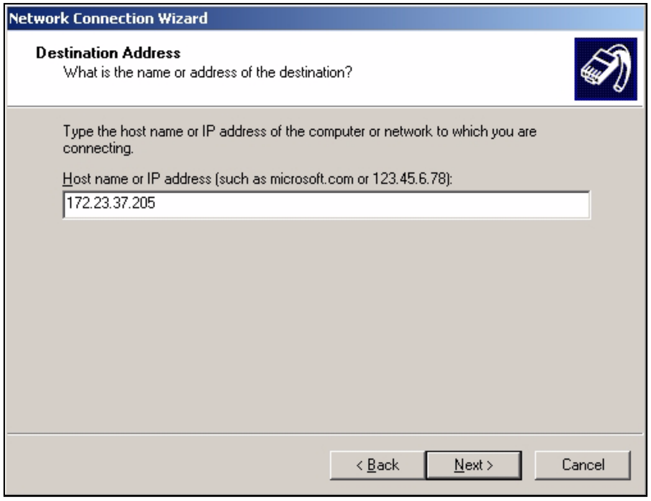
○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

< Back
Next >
Cancel

3 Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the ZyWALL is using for L2TP VPN. Click **Next**.

Figure 286 New Connection Wizard: Destination Address



Network Connection Wizard

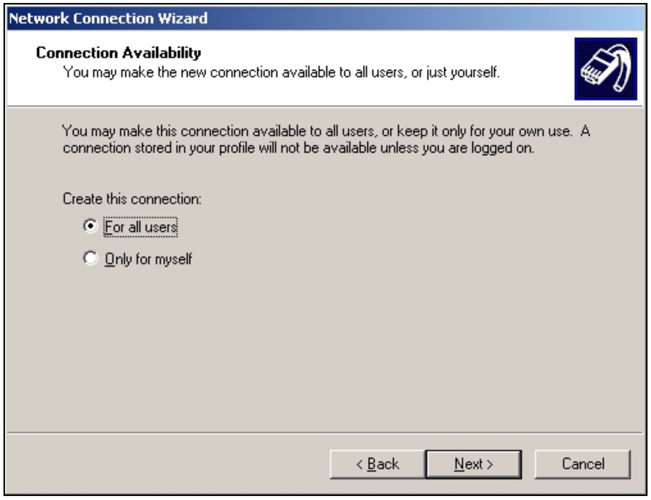
Destination Address
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):
172.23.37.205

4 Select **For all users** and click **Next**.

Figure 287 New Connection Wizard: Connection Availability



Network Connection Wizard

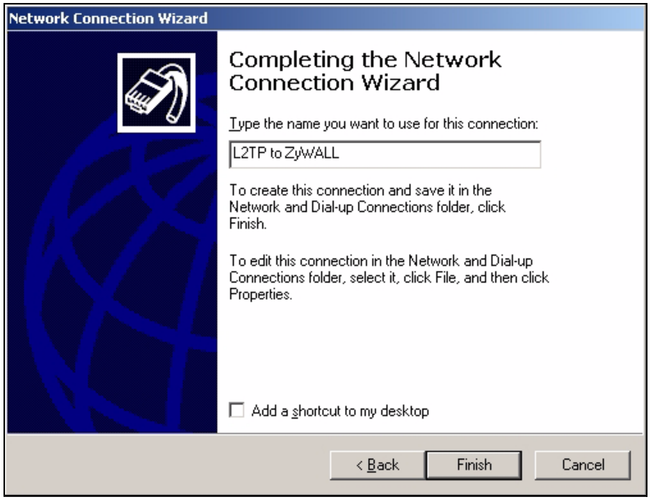
Connection Availability
You may make the new connection available to all users, or just yourself.

You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:
● For all users
○ Only for myself

5 Name the connection **L2TP to ZyWALL** and click **Finish**.

Figure 288 New Connection Wizard: Naming the Connection



Network Connection Wizard

Completing the Network Connection Wizard

Type the name you want to use for this connection:
L2TP to ZyWALL

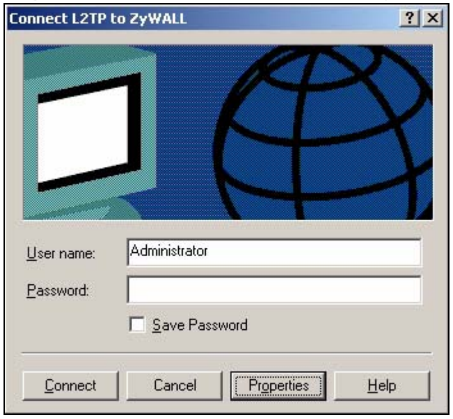
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.

☐ Add a shortcut to my desktop

6 Click **Properties**.

Figure 289 Connect L2TP to ZyWALL


Connect L2TP to ZyWALL
?
X
Connect
Cancel
Properties
Help

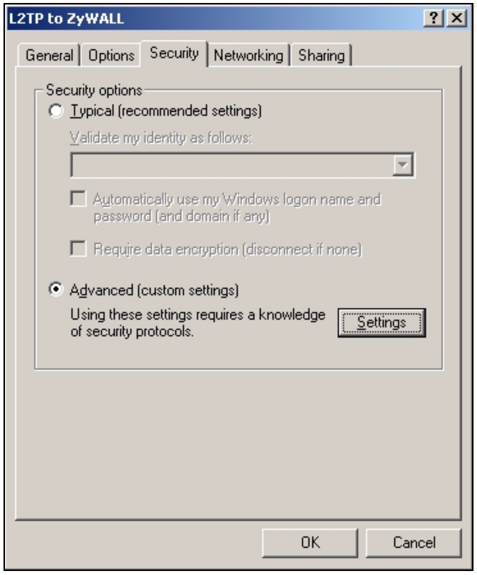
User name: Administrator

Password:

☐ Save Password

7 Click **Security** and select **Advanced (custom settings)** and click **Settings**.

Figure 290 Connect L2TP to ZyWALL: Security


L2TP to ZyWALL
?
X
General
Options
Security
Networking
Sharing
Settings
OK
Cancel

Security options

○ Typical (recommended settings)

Validate my identity as follows:

☐ Automatically use my Windows logon name and password (and domain if any)

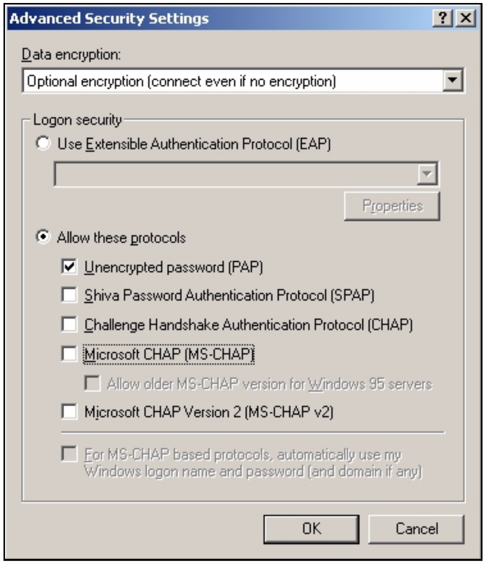
☐ Require data encryption (disconnect if none)

● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

8 Select **Optional encryption allowed (connect even if no encryption)** and the **Allow these protocols** radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**. Click **Yes** if a screen pops up.

Figure 291 Connect L2TP to ZyWALL: Security > Advanced



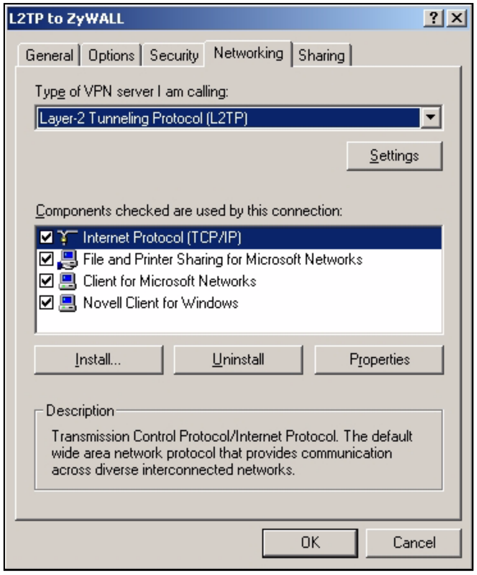
Advanced Security Settings
? ×
Properties
OK
Cancel

Data encryption:
Optional encryption (connect even if no encryption)

Logon security
○ Use Extensible Authentication Protocol (EAP)
● Allow these protocols
☑ Unencrypted password (PAP)
☐ Shiva Password Authentication Protocol (SPAP)
☐ Challenge Handshake Authentication Protocol (CHAP)
☐ Microsoft CHAP (MS-CHAP)
☐ Allow older MS-CHAP version for Windows 95 servers
☐ Microsoft CHAP Version 2 (MS-CHAP v2)
☐ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

9 Click **Networking** and select **Layer 2 Tunneling Protocol (L2TP)** from the drop-down list box. Click **OK**.

Figure 292 Connect L2TP to ZyWALL: Networking



L2TP to ZyWALL
? ×
General
Options
Security
Networking
Sharing
Settings
Install...
Uninstall
Properties
OK
Cancel

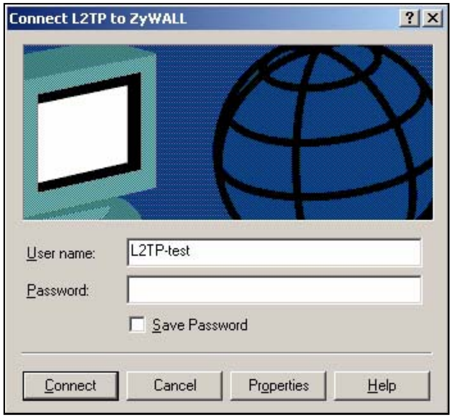
Type of VPN server I am calling:
Layer-2 Tunneling Protocol (L2TP)

Components checked are used by this connection:
☑ Internet Protocol (TCP/IP)
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks
☑ Novell Client for Windows

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

10 Enter your user name and password and click **Connect**. It may take up to one minute to establish the connection and register on the network.

Figure 293 Connect L2TP to ZyWALL


Connect L2TP to ZyWALL
Connect
Cancel
Properties
Help

User name: L2TP-test

Password:

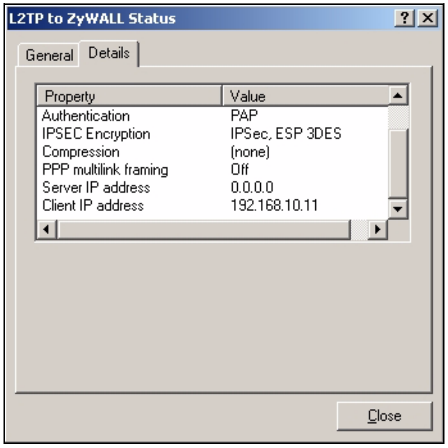
☐ Save Password

11 A ZyWALL-L2TP icon displays in your system tray. Double-click it to open a status screen.

Figure 294 ZyWALL-L2TP System Tray Icon

12 Click **Details** and scroll down to see the address that you received is from the L2TP range you specified on the ZyWALL (192.168.10.10-192.168.10.20).

Figure 295 L2TP to ZyWALL Status: Details


L2TP to ZyWALL Status
General
Details
Close

Property	Value
Authentication	PAP
IPSEC Encryption	IPSec, ESP 3DES
Compression	(none)
PPP multilink framing	Off
Server IP address	0.0.0.0
Client IP address	192.168.10.11

13 Access a server or other network resource behind the ZyWALL to make sure your access works.

PART IV

Application Patrol & Anti-X

Application Patrol (379)
Anti-Virus (403)
IDP (417)
ADP (445)
Content Filter Screens (463)
Content Filter Reports (483)

27

Application Patrol

This chapter describes how to use application patrol for the ZyWALL. It provides an overview first and then introduces the screens. See Section 5.4.13 on page 119 for related information on these screens.

27.1 Application Patrol Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, http and ftp) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

The ZyWALL checks firewall rules before it checks application patrol rules for traffic going through the ZyWALL.

If you want to use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

Application patrol examines every TCP and UDP connection passing through the ZyWALL and identifies what application is using the connection. Then, you can specify, by application, whether or not the ZyWALL continues to route the connection.

27.2 Classification of Applications

There are two ways the ZyWALL can identify the application. The first approach is called auto. In this approach, the ZyWALL looks at the IP payload (OSI level-7) and attempts to match it with known patterns for specific applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the ZyWALL examines several packets to make sure the match is correct.

The ZyWALL allows the first eight packets to go through the firewall, regardless of the application patrol policy for the application. The ZyWALL examines these first eight packets to identify the application.

The second approach is called service ports. In this approach, the ZyWALL only uses OSI level-3 information, such as IP address and port, to identify what application is using the connection. This approach is available in case the ZyWALL identifies a lot of "false positives" for a particular application.

27.3 Configurable Application Policies

The ZyWALL has policies for individual applications. For each policy, you can specify the default action the ZyWALL takes once it identifies one of the service's connections.

- **Forward** - the ZyWALL routes the packets for this application.
- **Drop** - the ZyWALL does not route the packets for this application, and it does not notify the client of this decision.
- **Reject** - the ZyWALL does not route the packets for this application, and it notifies the client of this decision.

You can also specify custom policies that have the ZyWALL forward, drop, or reject a service's connections based on criteria that you specify (like the source zone, destination zone, original destination port of the connection, schedule, user, source, and destination information). Your custom policies take priority over the policy's default settings.

27.4 Bandwidth Management

When you allow an application, you can restrict the bandwidth it uses or even the bandwidth that particular features in the application (like voice, video, or file sharing) use. This restriction may be ineffective in certain cases, however, such as using MSN to send files via P2P.

The application patrol bandwidth management is more flexible and powerful than the bandwidth management in policy routes. Application patrol controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Bandwidth management in policy routes has priority over application patrol bandwidth management. It is recommended to use application patrol bandwidth management for TCP and UDP traffic and remove it from the policy routes.

27.4.1 Connection and Packet Directions

Application patrol looks at the connection direction, that is from which zone the connection was initiated and to which zone the connection is going.

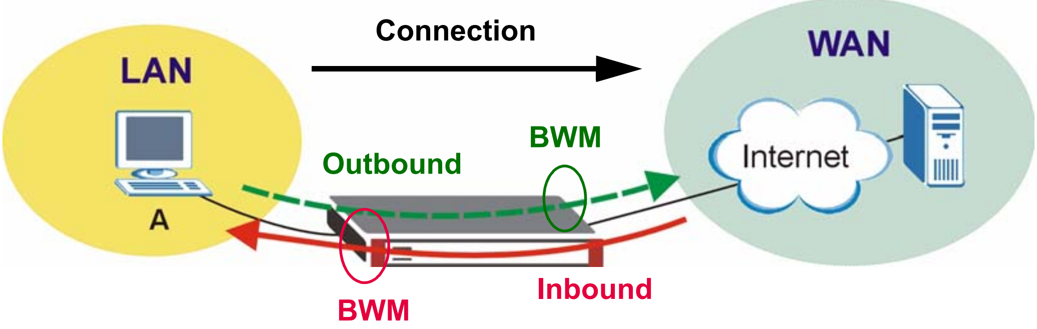
A connection has outbound and inbound packet flows. The ZyWALL controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN to WAN connection is initiated from the LAN and goes to the WAN.

- Outbound traffic goes from a LAN zone device to a WAN zone device. Bandwidth management is applied before sending the packets out a WAN zone interface on the ZyWALL.
- Inbound traffic comes back from the WAN zone device to the LAN zone device. Bandwidth management is applied before sending the traffic out a LAN zone interface.

Figure 296 LAN to WAN Connection and Packet Directions



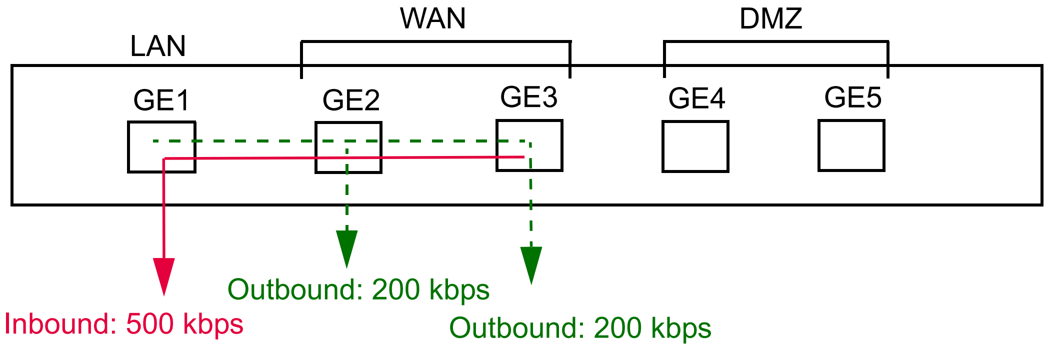
27.4.2 Outbound and Inbound Bandwidth Limits

You can limit an application’s outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface’s bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit.

Take a LAN to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN so outbound means the traffic traveling from the LAN to the WAN. Each of the WAN zone’s two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN so inbound means the traffic traveling from the WAN to the LAN.

Figure 297 LAN to WAN, Outbound 200 kbps, Inbound 500 kbps



27.4.3 Bandwidth Management Priority

The ZyWALL gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.

Then lower-priority traffic gets bandwidth.

The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.

The ZyWALL automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

27.4.4 Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

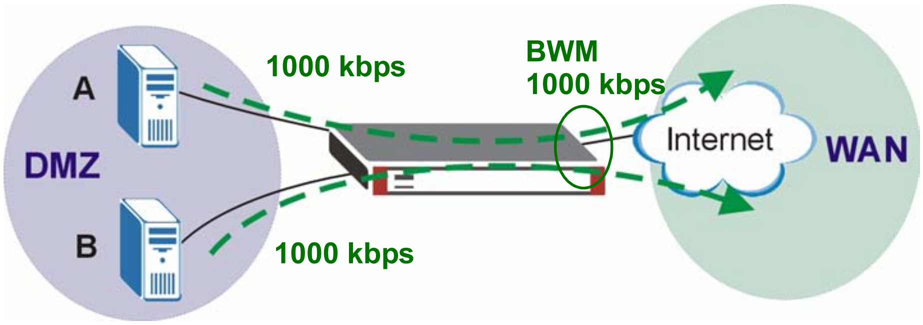
After each application gets its configured bandwidth rate, the ZyWALL uses the fairness-based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

27.4.5 Bandwidth Management Behavior

This section shows how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers **A** and **B**. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**’s traffic and policy B for server **B**’s traffic.

Figure 298 Bandwidth Management Behavior



27.4.5.1 Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 108 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

27.4.5.2 Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps that server **B** can use.

Table 109 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

27.4.5.3 Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the ZyWALL divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 110 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

27.4.5.4 Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the ZyWALL still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

Table 111 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

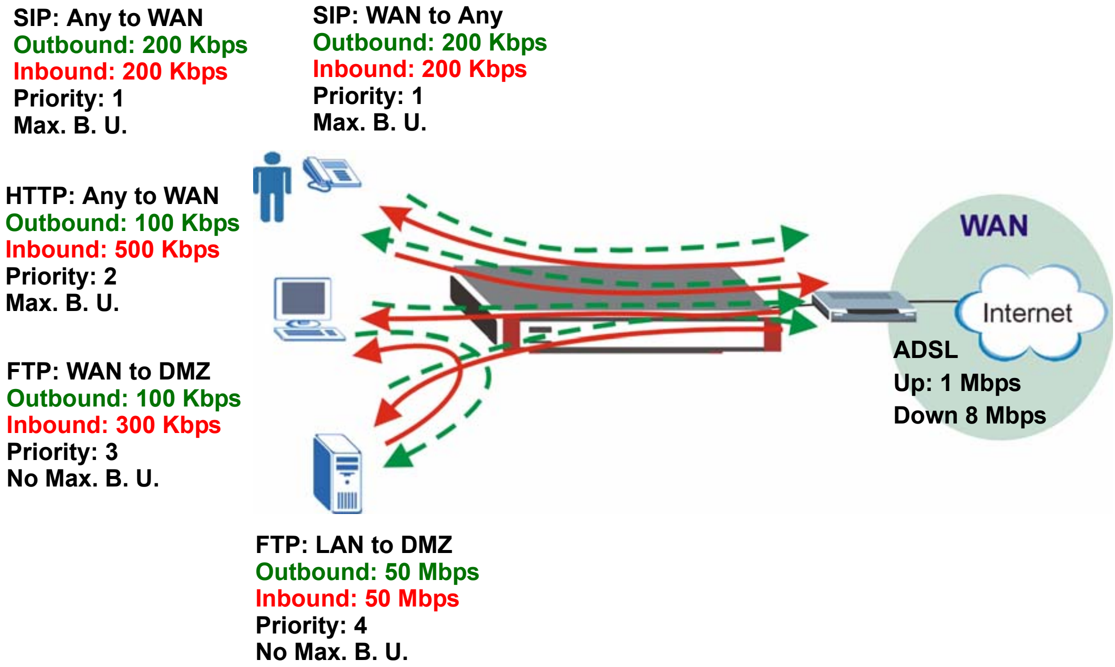
27.5 Application Patrol Bandwidth Management Examples

Bandwidth management is very useful when applications are competing for limited bandwidth. For example, say you have a WAN zone interface connected to an ADSL device with a 8 Mbps downstream and 1 Mbps upstream ADSL connection. The following sections give some simplified examples of using application patrol policies to manage applications competing for that 1 Mbps of upstream bandwidth.

Here is an overview of what the rules need to accomplish. See the following sections for more details.

- SIP traffic from VIP users must get through with the least possible delay regardless of if it is an outgoing call or an incoming call. The VIP users must be able to make and receive SIP calls no matter which interface they are connected to.
- HTTP traffic needs to be given priority over FTP traffic.
- FTP traffic from the WAN to the DMZ must be limited so it does not interfere with SIP and HTTP traffic.
- FTP traffic from the LAN to the DMZ can use more bandwidth since the interfaces support up to 1 Gbps connections, but it must be the lowest priority and limited so it does not interfere with SIP and HTTP traffic.

Figure 299 Application Patrol Bandwidth Management Example


SIP: Any to WAN
Outbound: 200 Kbps
Inbound: 200 Kbps
Priority: 1
Max. B. U.
SIP: WAN to Any
Outbound: 200 Kbps
Inbound: 200 Kbps
Priority: 1
Max. B. U.
HTTP: Any to WAN
Outbound: 100 Kbps
Inbound: 500 Kbps
Priority: 2
Max. B. U.
FTP: WAN to DMZ
Outbound: 100 Kbps
Inbound: 300 Kbps
Priority: 3
No Max. B. U.
WAN
Internet
ADSL
Up: 1 Mbps
Down 8 Mbps
FTP: LAN to DMZ
Outbound: 50 Mbps
Inbound: 50 Mbps
Priority: 4
No Max. B. U.

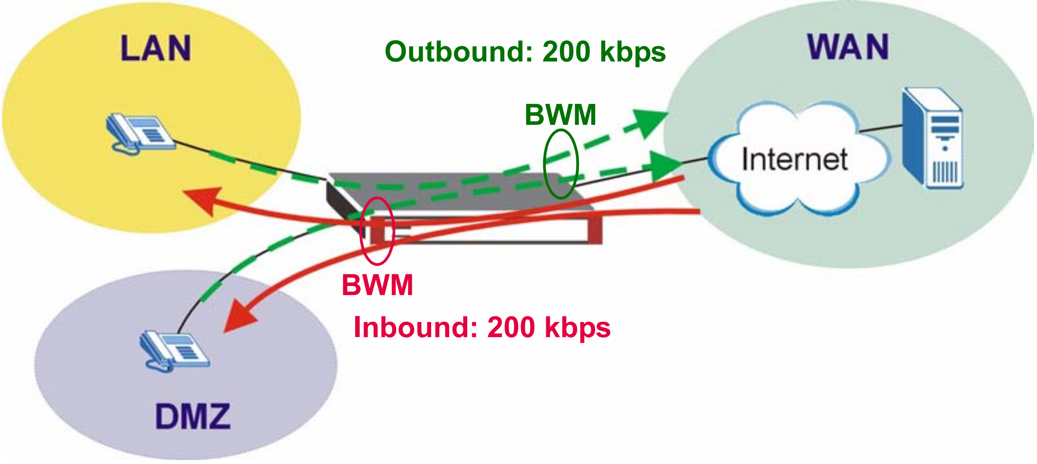
27.5.1 Setting the Interface’s Bandwidth

Use the interface screens to set the WAN zone interface’s upstream bandwidth to be equal to (or slightly less than) what the connected device can support. This example uses 1000 Kbps.

27.5.2 SIP Any to WAN Bandwidth Management Example

- Manage SIP traffic going to the WAN zone from a VIP user on the LAN or DMZ.
- Outbound traffic (to the WAN from the LAN and DMZ) is limited to 200 kbps. The ZyWALL applies this limit before sending the traffic to the WAN.
- Inbound traffic (to the LAN and DMZ from the WAN) is also limited to 200 kbps. The ZyWALL applies this limit before sending the traffic to LAN or DMZ.
- Highest priority (1). Set policies for other applications to lower priorities so the SIP traffic always gets the best treatment.
- Enable maximize bandwidth usage so the SIP traffic can borrow unused bandwidth.

Figure 300 SIP Any to WAN Bandwidth Management Example


LAN
Outbound: 200 kbps
WAN
BWM
Internet
BWM
Inbound: 200 kbps
DMZ

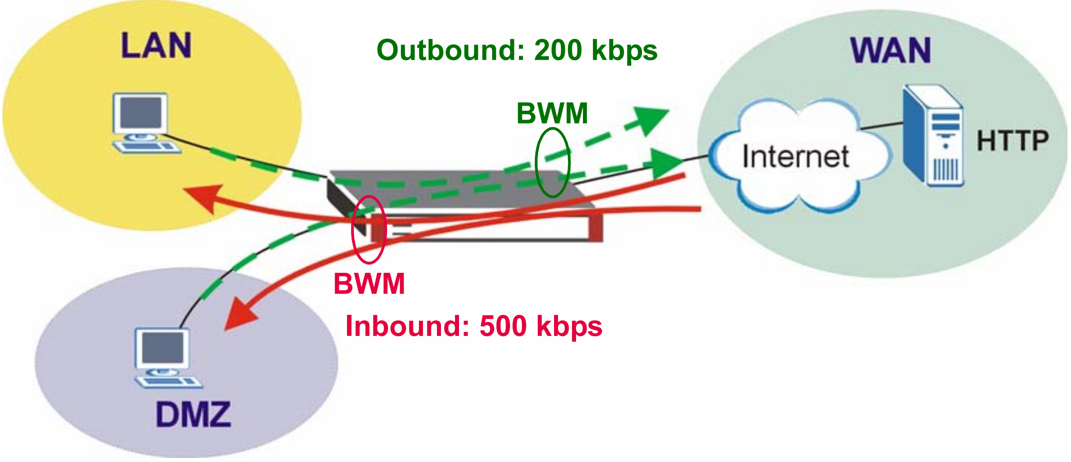
27.5.3 SIP WAN to Any Bandwidth Management Example

You also create a policy for calls coming in from the SIP server on the WAN. It is the same as the SIP Any to WAN policy, but with the directions reversed (WAN to Any instead of Any to WAN).

27.5.4 HTTP Any to WAN Bandwidth Management Example

- Inbound traffic gets more bandwidth as the local users will probably download more than they upload (and the ADSL connection supports this).
- Second highest priority (2). Set policies for other applications (except SIP) to lower priorities so the local users' HTTP traffic gets sent before non-SIP traffic.
- Enable maximize bandwidth usage so the HTTP traffic can borrow unused bandwidth.

Figure 301 HTTP Any to WAN Bandwidth Management Example

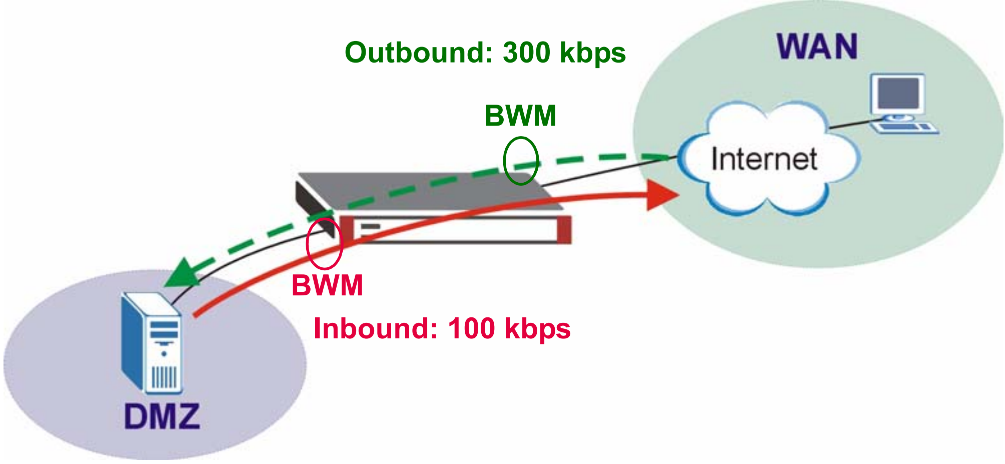

LAN
Outbound: 200 kbps
WAN
BWM
Internet
HTTP
BWM
Inbound: 500 kbps
DMZ

27.5.5 FTP WAN to DMZ Bandwidth Management Example

- ADSL supports more downstream than upstream so you allow remote users 300 kbps for uploads to the DMZ FTP server (outbound) but only 100 kbps for downloads (inbound).

- Third highest priority (3).
- Disable maximize bandwidth usage since you do not want to give FTP more bandwidth.

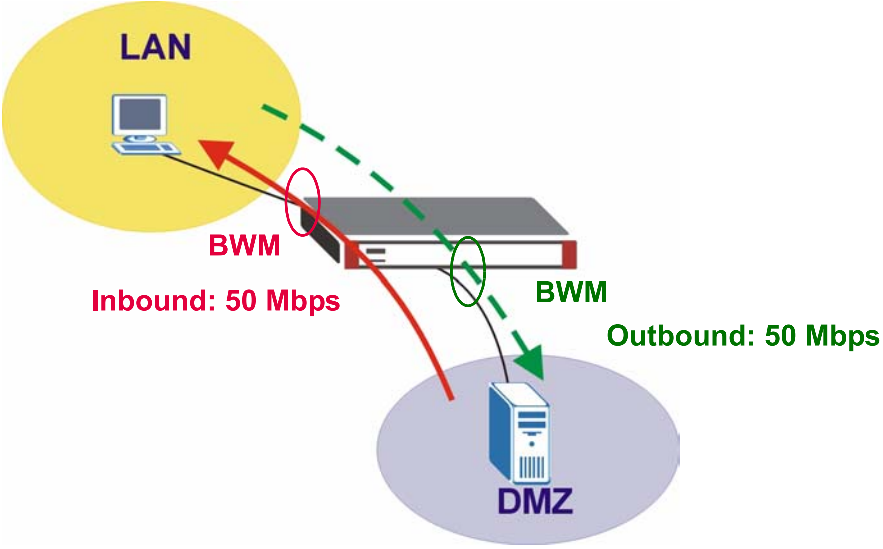
Figure 302 FTP WAN to DMZ Bandwidth Management Example


Outbound: 300 kbps
WAN
BWM
Internet
BWM
Inbound: 100 kbps
DMZ

27.5.6 FTP LAN to DMZ Bandwidth Management Example

- The LAN and DMZ zone interfaces are connected to Ethernet networks (not an ADSL device) so you limit both outbound and inbound traffic to 50 Mbps.
- Fourth highest priority (4).
- Disable maximize bandwidth usage since you do not want to give FTP more bandwidth.

Figure 303 FTP LAN to DMZ Bandwidth Management Example


LAN
BWM
Inbound: 50 Mbps
BWM
Outbound: 50 Mbps
DMZ

27.6 Other Applications

Sometimes, the ZyWALL cannot identify the application. For example, the application might be a new application, or the packets might arrive out of sequence. (The ZyWALL does not reorder packets when identifying the application.) In these cases, you can still provide a default rule for the ZyWALL to follow. You can use source zone, destination zone, destination port, schedule, user, source, and destination information as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify what the ZyWALL should do more precisely. You can also control the bandwidth used by these other applications.

27.7 Application Patrol Screens

Use the **General** summary screen to enable and disable application patrol.

Use the **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, and **Streaming** screens to look at the applications the ZyWALL can recognize, and review the settings for each one. You can also enable and disable the rules for each application and specify the default and custom policies for each application.

The **Other** screen controls what the ZyWALL does when it does not recognize the application, and it identifies the conditions that refine this. It also lets you open the **Other Configuration Add/Edit** screen to create new conditions or edit existing ones.

Use the **Statistics** screen to see a bandwidth usage graph and statistics for each protocol.

27.8 Application Patrol General

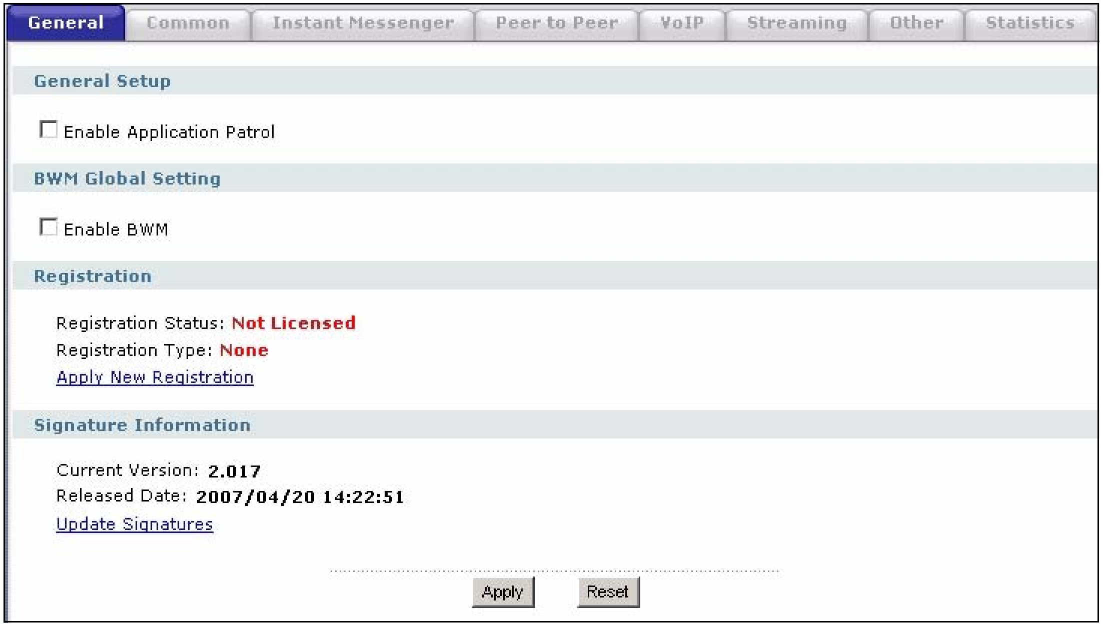
Use this screen to enable and disable application patrol. It also lists the registration status and details about the signature set the ZyWALL is using.

You must register for the IDP/AppPatrol signature service (at least the trial) before you can use it.

See Chapter 8 on page 165 for how to register.

Click **AppPatrol** to open the following screen.

Figure 304 AppPatrol > General


General
Common
Instant Messenger
Peer to Peer
VoIP
Streaming
Other
Statistics
General Setup
☐ Enable Application Patrol
BWM Global Setting
☐ Enable BWM
Registration
Apply New Registration
Signature Information
Update Signatures
Apply
Reset

Registration Status: Not Licensed
Registration Type: None

Current Version: 2.017
Released Date: 2007/04/20 14:22:51

The following table describes the labels in this screen. See Section 27.9.1 on page 391 for more information as well.

Table 112 AppPatrol > General

LABEL	DESCRIPTION
Enable Application Patrol	Select this check box to turn on application patrol.
Enable BWM	This is a global setting for enabling or disabling bandwidth management on the ZyWALL. You must enable this setting to have individual policy routes or application patrol policies apply bandwidth management. This same setting also appears in the **Network > Routing > Policy Route** screen. Enabling or disabling it in one screen also enables or disables it in the other screen.
Registration	The following fields display information about the current state of your subscription for IDP/application patrol signatures.
Registration Status	This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**).
Registration Type	This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard’s PIN number (**Standard**). **None** displays when the service is not activated.
Apply new Registration	This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service.
Signature Information	The following fields display information on the current signature set that the ZyWALL is using.
Current Version	This field displays the IDP signature and anomaly rule set version number. This number gets larger as the set is enhanced.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.

Table 112 AppPatrol > General (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

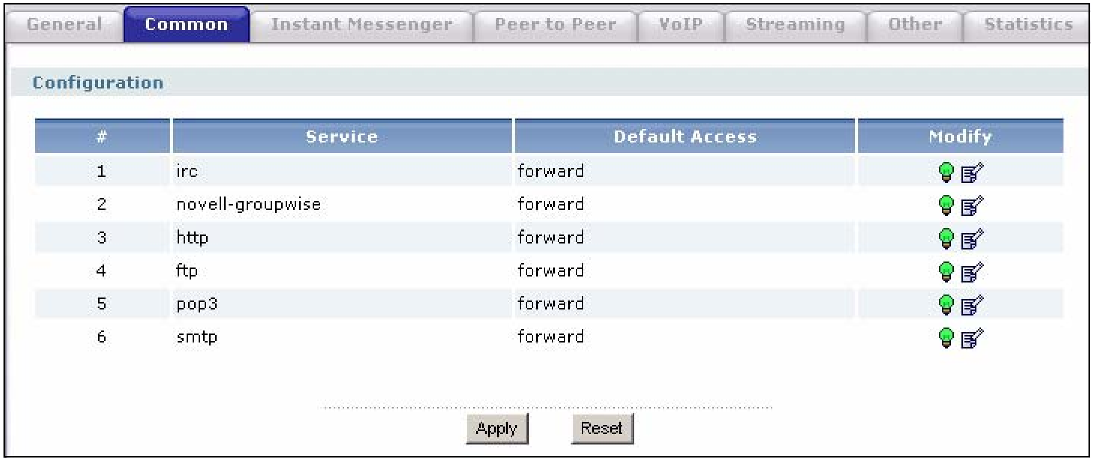
27.9 Application Patrol Applications

Use the application patrol **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, or **Streaming** screen to manage traffic of individual applications.

Use the **Common** screen (shown here as an example) to manage traffic of the most commonly used web, file transfer and e-mail protocols.

Click **AppPatrol** > **Common** to open the following screen.

Figure 305 AppPatrol > Common



#	Service	Default Access	Modify
1	irc	forward	
2	novell-groupwise	forward	
3	http	forward	
4	ftp	forward	
5	pop3	forward	
6	smtp	forward	

The following table describes the labels in this screen. See Section 27.9.1 on page 391 for more information as well.

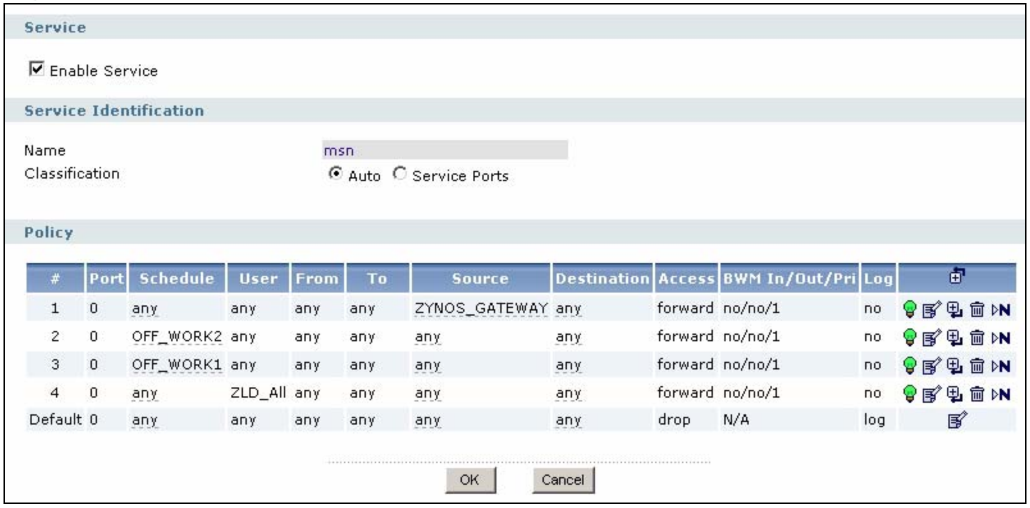
Table 113 AppPatrol > Common

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific application.
Service	This field displays the name of the application.
Default Access	This field displays what the ZyWALL does with packets for this application. Choices are: **forward**, **drop**, and **reject**.
Modify	This column provides icons to activate and deactivate each application and to edit the settings for each one. To activate or deactivate patrol for an application, click the **Active** icon for the corresponding application. Make sure you click **Apply** to save and apply the change. To edit the settings for an application, click the **Edit** icon next to the application. The **Configuration Edit** screen appears.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

27.9.1 Application Patrol Edit

Use this screen to edit the settings for an application. To access this screen, go to the application patrol **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, or **Streaming** screen and click an application's **Edit** icon. The screen displayed here is for the MSN instant messenger service.

Figure 306 Application Edit



Service

☑ Enable Service

Service Identification

Name: msn

Classification: ● Auto ○ Service Ports

Policy

#	Port	Schedule	User	From	To	Source	Destination	Access	BWM In/Out/Pri	Log
1	0	any	any	any	any	ZYNOS_GATEWAY	any	forward	no/no/1	no
2	0	OFF_WORK2	any	any	any	any	any	forward	no/no/1	no
3	0	OFF_WORK1	any	any	any	any	any	forward	no/no/1	no
4	0	any	ZLD_All	any	any	any	any	forward	no/no/1	no
Default	0	any	any	any	any	any	any	drop	N/A	log

The following table describes the labels in this screen.

Table 114 Application Edit

LABEL	DESCRIPTION
Service	
Enable Service	Select this check box to turn on patrol for this application.
Service Identification	
Name	This field displays the name of the application.
Classification	Specify how the ZyWALL should identify this application. Choices are: **Auto** - the ZyWALL identifies this application by matching the IP payload with the application's pattern(s). **Service Ports** - the ZyWALL identifies this application by looking at the destination port in the IP header.
Service Port	This is available if the **Classification** is **Service Ports**. You can view and edit the ports used to identify this application.
Add icon	When the **Classification** is **Service Ports**, this column provides icons to add and remove port numbers used to identify the application. Click **Add** add a port number. Type the destination port number in the **Service Port** field. Click **Remove** to delete a port number. The web configurator confirms that you want to delete the port number before doing so.
Policy	This table lists the policies configured for this application.

Table 114 Application Edit (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific condition. Note: The ZyWALL checks conditions in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the ZyWALL by putting more common conditions at the top of the list.
Port	This field displays the specific port number to which this policy applies.
Schedule	This is the schedule that defines when the policy applies. **any** means the policy is active at all times if enabled.
User	This is the user name or user group to which the policy applies. If **any** displays, the policy applies to all users.
From	This is the source zone of the traffic to which this policy applies.
To	This is the destination zone of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If **any** displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If **any** displays, the policy is effective for every destination.
Access	This field displays what the ZyWALL does with packets for this application that match this policy. **forward** - the ZyWALL routes the packets for this application. **Drop** - the ZyWALL does not route the packets for this application and does not notify the client of its decision. **Reject** - the ZyWALL does not route the packets for this application and notifies the client of its decision.
BWM	These fields show the amount of bandwidth the application's traffic that matches the policy can use. These fields only apply when **Access** is set to **forward**. **In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the application to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the application's incoming traffic. **Out** - This is how much outbound bandwidth, in kilobits per second, this policy allows the application to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the application's outgoing traffic. **Pri** - This is the priority for this application's traffic that matches this policy. The smaller the number, the higher the priority. The traffic of an application with higher priority is given bandwidth before traffic of an application with lower priority. The ZyWALL ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Log	This field shows whether the ZyWALL generates a log (**log**), a log and alert (**log alert**) or neither (**no**) when the application's traffic matches this policy.

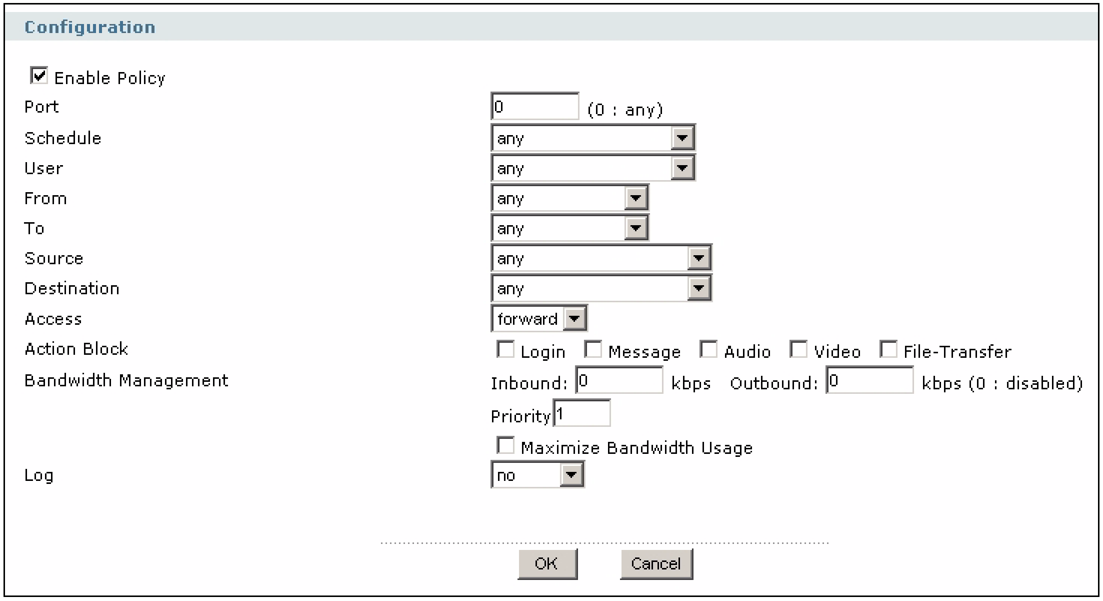
Table 114 Application Edit (continued)

LABEL	DESCRIPTION
Add icon	Click the **Add** icon in the heading row to add a new first entry. The **Active** icon displays whether the entry is enabled or not. Click the **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Add** icon in an entry to add a new entry below the current entry. Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. To move an entry up or down in the list, click on the **Move to N** icon next to the entry, and type the line number (**#** field) of where you want to move the entry. The **#** field is updated accordingly. The ordering of the entries is important as they are applied in order of their numbering.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.9.2 Application Patrol Policy Edit

The **Application Policy Edit** screen allows you to edit a group of settings for an application. To access this screen, go to the application patrol **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, or **Streaming** screen and click an application's **Edit** icon. Then click the **Add** icon or an **Edit** icon in the **Policy** table. The screen displayed here is for the MSN instant messenger service.

Figure 307 Application Policy Edit



Configuration

☑ Enable Policy
Port 0 (0 : any)
Schedule any
User any
From any
To any
Source any
Destination any
Access forward
Action Block ☐ Login ☐ Message ☐ Audio ☐ Video ☐ File-Transfer
Bandwidth Management Inbound: 0 kbps Outbound: 0 kbps (0 : disabled)
Priority 1
☐ Maximize Bandwidth Usage
Log no

The following table describes the labels in this screen.

Table 115 Application Policy Edit

LABEL	DESCRIPTION
Enable Policy	Select this check box to turn on this policy for the application.
Port	Use this field to specify a specific port number to which to apply this policy. Type zero, if this policy applies for every port number.

Table 115 Application Policy Edit (continued)

LABEL	DESCRIPTION
Schedule	Select a schedule that defines when the policy applies or select **Create Object** to configure a new one (see Chapter 37 on page 527 for details). Otherwise, select **none** to make the policy always effective.
User	Select a user name or user group to which to apply the policy. Select **Create Object** to configure a new user account (see Section 34.2.1 on page 506 for details). Select **any** to apply the policy for every user.
From	Select the source zone of the traffic to which this policy applies.
To	Select the destination zone of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every destination.
Access	This field controls what the ZyWALL does with packets for this application that match this policy. Choices are: **forward** - the ZyWALL routes the packets for this application. **Drop** - the ZyWALL does not route the packets for this application and does not notify the client of its decision. **Reject** - the ZyWALL does not route the packets for this application and notifies the client of its decision.
Action Block	For some applications, you can select individual uses of the application that the policy will have the ZyWALL block. These fields only apply when **Access** is set to **forward**. **Login** - Select this option to block users from logging in to a server for this application. **Message** - Select this option to block users from sending or receiving instant messages. **Audio** - Select this option to block users from sending or receiving audio traffic. **Video** - Select this option to block users from sending or receiving video traffic. **File Transfer** - Select this option to block users from sending or receiving files.
Bandwidth Management	Configure these fields to set the amount of bandwidth the application can use. These fields only apply when **Access** is set to **forward**. You must also enable bandwidth management in the main application patrol screen (**AppPatrol > General**) in order to apply bandwidth shaping.
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the application to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the application's traffic that the ZyWALL sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.

Table 115 Application Policy Edit (continued)

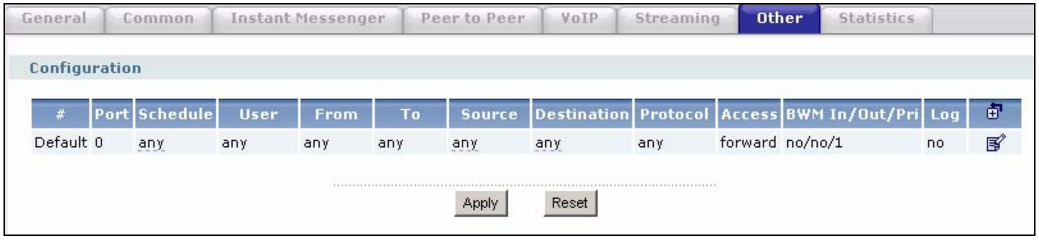
LABEL	DESCRIPTION
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the application to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the application's traffic that the ZyWALL sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Priority	Enter a number between 1 and 7 to set the priority for this application's traffic that matches this policy. The smaller the number, the higher the priority. The ZyWALL gives traffic of an application with higher priority bandwidth before traffic of an application with lower priority. The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth between applications with the same priority. The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Maximize Bandwidth Usage	Enable maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface. After each application gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when the application's traffic matches this policy. See Chapter 46 on page 625 for more on logs.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.10 Other Protocol Screen

The **Other Protocol** screen controls the default policy for TCP and UDP traffic that the ZyWALL cannot identify. In other words, you can control what the ZyWALL does when it does not recognize the application. This screen also allows you to add, edit, and remove conditions to this default policy.

Click **AppPatrol** > **Other** to open the **Other Protocol** screen.

Figure 308 AppPatrol > Other



#	Port	Schedule	User	From	To	Source	Destination	Protocol	Access	BWM In/Out/Pri	Log	
Default	0	any	any	any	any	any	any	any	forward	no/no/1	no	

The following table describes the labels in this screen. See Section 27.10.1 on page 397 for more information as well.

Table 116 AppPatrol > Other

LABEL	DESCRIPTION
Policy	This table lists the policies configured for traffic which does not match an application.
#	This field is a sequential value, and it is not associated with a specific condition. Note: The ZyWALL checks conditions in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the ZyWALL by putting more common conditions at the top of the list.
Port	This field displays the specific port number to which this policy applies.
Schedule	This is the schedule that defines when the policy applies. **any** means the policy always applies.
User	This is the user name or user group to which the policy applies. If **any** displays, the policy applies to all users.
From	This is the source zone of the traffic to which this policy applies.
To	This is the destination zone of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If **any** displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If **any** displays, the policy is effective for every destination.
Protocol	This is the protocol of the traffic to which this policy applies.
Access	This field displays what the ZyWALL does with packets that match this policy. **forward** - the ZyWALL routes the packets. **Drop** - the ZyWALL does not route the packets and does not notify the client of its decision. **Reject** - the ZyWALL does not route the packets and notifies the client of its decision.
BWM	These fields show the amount of bandwidth the traffic can use. These fields only apply when **Access** is set to **forward**. **In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the ZyWALL sends to a connection’s initiator. If **no** displays here, this policy does not apply bandwidth management for the inbound traffic. **Out** - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the ZyWALL sends out from a connection’s initiator. If **no** displays here, this policy does not apply bandwidth management for the outbound traffic. **Pri** - This is the priority for the traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ZyWALL ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field’s configuration.
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this policy. See Chapter 46 on page 625 for more on logs.

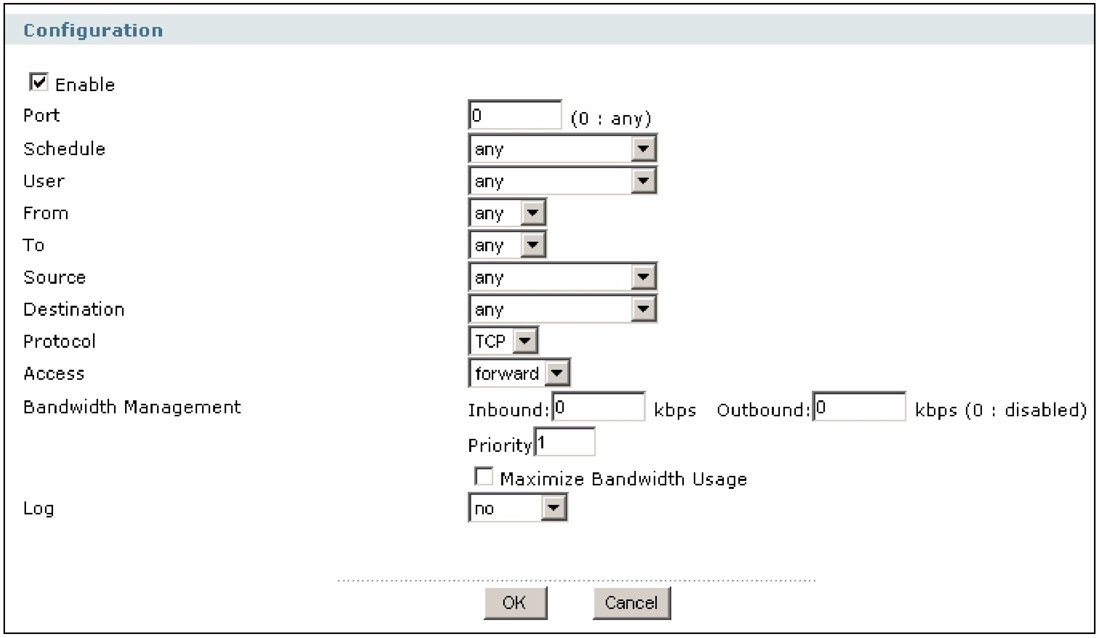
Table 116 AppPatrol > Other (continued)

LABEL	DESCRIPTION
Add icon	Click the **Add** icon in the heading row to add a new first entry. The **Active** icon displays whether the entry is enabled or not. Click the **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Add** icon in an entry to add a new entry below the current entry. Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. To move an entry up or down in the list, click on the **Move to N** icon next to the entry, and type the line number (**#** field) of where you want to move the entry. The **#** field is updated accordingly. The ordering of the entries is important as they are applied in order of their numbering.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

27.10.1 Other Configuration Add/Edit

The **Other Configuration Add/Edit** screen allows you to create a new condition or edit an existing one. To access this screen, go to the **Other Protocol** screen (see Section 27.10 on page 395), and click either the **Add** icon or an **Edit** icon.

Figure 309 AppPatrol > Other > Edit



☑ Enable
Port 0 (0 : any)
Schedule any
User any
From any
To any
Source any
Destination any
Protocol TCP
Access forward
Bandwidth Management Inbound: 0 kbps Outbound: 0 kbps (0 : disabled)
Priority 1
☐ Maximize Bandwidth Usage
Log no

The following table describes the labels in this screen.

Table 117 AppPatrol > Other > Edit

LABEL	DESCRIPTION
Enable	Select this check box to turn on this policy.
Port	Use this field to specify a specific port number to which to apply this policy. Type zero, if this policy applies for every port number.

Table 117 AppPatrol > Other > Edit (continued)

LABEL	DESCRIPTION
Schedule	Select a schedule that defines when the policy applies or select **Create Object** to configure a new one (see Chapter 37 on page 527 for details). Otherwise, select **any** to make the policy always effective.
User	Select a user name or user group to which to apply the policy. Select **Create Object** to configure a new user account (see Section 34.2.1 on page 506 for details). Select **any** to apply the policy for every user.
From	Select the source zone of the traffic to which this policy applies.
To	Select the destination zone of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every destination.
Protocol	Select the protocol for which this condition applies. Choices are: **TCP** and **UDP**. Select **any** to apply the policy to both TCP and UDP traffic.
Access	This field controls what the ZyWALL does with packets that match this policy. Choices are: **forward** - the ZyWALL routes the packets. **Drop** - the ZyWALL does not route the packets and does not notify the client of its decision. **Reject** - the ZyWALL does not route the packets and notifies the client of its decision.
Bandwidth Management	Configure these fields to set the amount of bandwidth the application can use. These fields only apply when **Access** is set to **forward**.
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ZyWALL sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ZyWALL sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.

Table 117 AppPatrol > Other > Edit (continued)

LABEL	DESCRIPTION
Priority	Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field’s configuration.
Maximize Bandwidth Usage	Enable maximize bandwidth usage to let the traffic matching this policy “borrow” any unused bandwidth on the out-going interface. After each application or type of traffic gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.
Log	This field controls what kind of record the ZyWALL creates when traffic matches this policy. Please see Chapter 46 on page 625 for more information. **no** - the ZyWALL does not record anything **log** - the ZyWALL creates a record in the log **log alert** - the ZyWALL creates an alert
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.11 Application Patrol Statistics

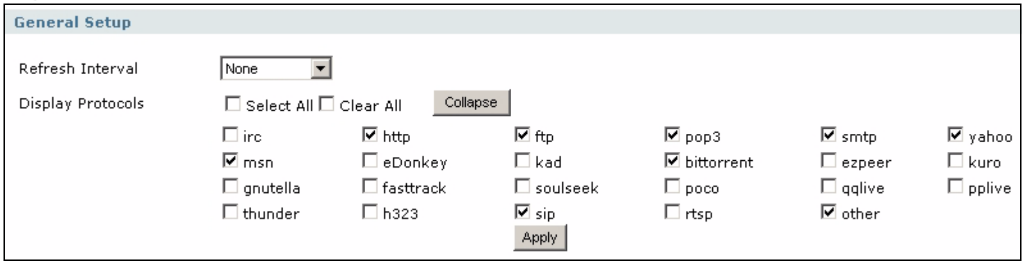
This screen displays a bandwidth usage graph and statistics for selected protocols.

Click **AppPatrol** > **Statistics** to open the following screen.

27.11.1 Application Patrol Statistics: General Setup

Use the top of the **AppPatrol** > **Statistics** screen to configure what to display.

Figure 310 AppPatrol > Statistics: General Setup



General Setup

Refresh Interval: None

Display Protocols: ☐ Select All ☐ Clear All

☐ irc	☑ http	☑ ftp	☑ pop3	☑ smtp	☑ yahoo
☑ msn	☐ eDonkey	☐ kad	☑ bittorrent	☐ ezpeer	☐ kuro
☐ gnutella	☐ fasttrack	☐ soulseek	☐ poco	☐ qqlive	☐ pplive
☐ thunder	☐ h323	☑ sip	☐ rtsp	☑ other	

The following table describes the labels in this screen.

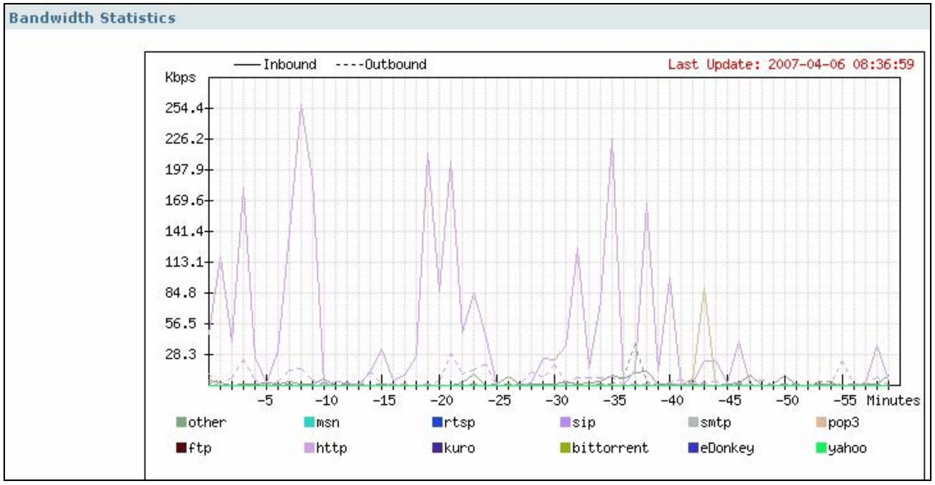
Table 118 AppPatrol > Statistics: General Setup

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the statistics display to update.
Display Protocols	Select the protocols for which to display statistics. **Select All** selects all of the protocols. **Clear All** clears all of the protocols. Click **Expand** to display individual protocols. **Collapse** hides them. Statistics for the selected protocols display after you click **Apply**.

27.11.2 Application Patrol Statistics: Bandwidth Statistics

The middle of the **AppPatrol** > **Statistics** screen displays a bandwidth usage line graph for the selected protocols.

Figure 311 AppPatrol > Statistics: Bandwidth Statistics

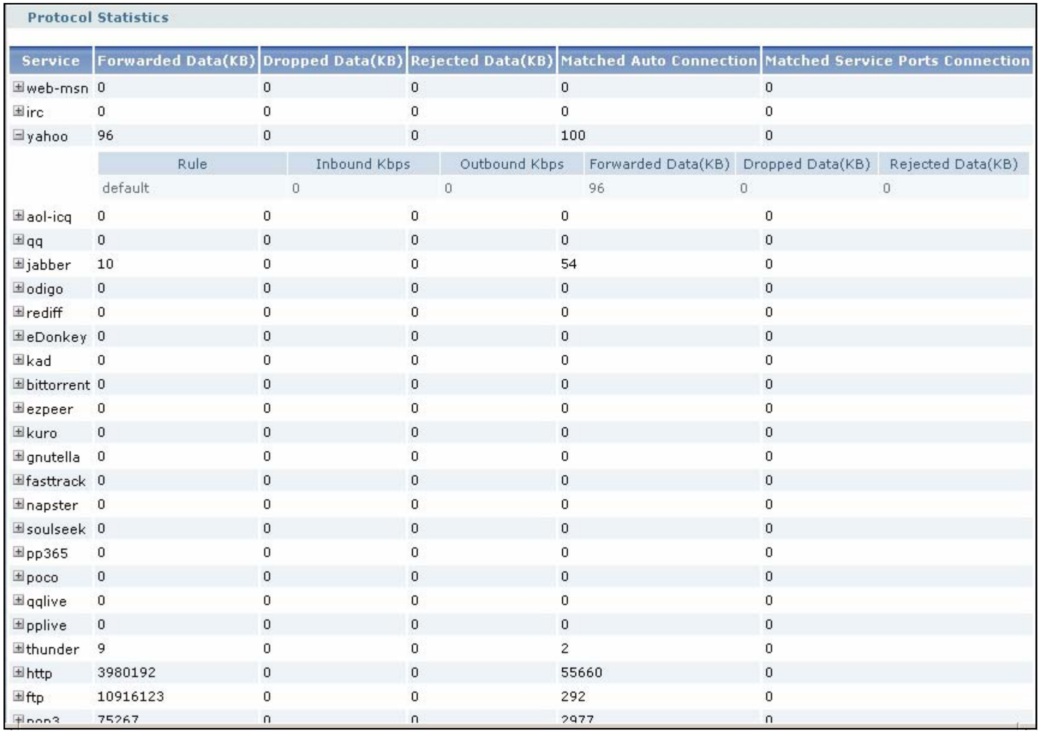

Bandwidth Statistics
Inbound
Outbound
Last Update: 2007-04-06 08:36:59
Kbps
254.4
226.2
197.9
169.6
141.4
113.1
84.8
56.5
28.3
-5
-10
-15
-20
-25
-30
-35
-40
-45
-50
-55
Minutes
other
msn
rtsp
sip
smtp
pop3
ftp
http
kuro
bittorrent
eDonkey
yahoo

- The y-axis represents the amount of bandwidth used.
- The x-axis shows the time period over which the bandwidth usage occurred.
- A solid line represents a protocol's incoming bandwidth usage. This is the protocol's traffic that the ZyWALL sends to the initiator of the connection.
- A dotted line represents a protocol's outgoing bandwidth usage. This is the protocol's traffic that the ZyWALL sends out from the initiator of the connection.
- Different colors represent different protocols.

27.11.3 Application Patrol Statistics: Protocol Statistics

The bottom of the **AppPatrol** > **Statistics** screen displays statistics for each of the selected protocols.

Figure 312 AppPatrol > Statistics: Protocol Statistics



Protocol Statistics

Service	Forwarded Data(KB)	Dropped Data(KB)	Rejected Data(KB)	Matched Auto Connection	Matched Service Ports Connection
⊞web-msn	0	0	0	0	0
⊞irc	0	0	0	0	0
⊟yahoo	96	0	0	100	0

Rule	Inbound Kbps	Outbound Kbps	Forwarded Data(KB)	Dropped Data(KB)	Rejected Data(KB)
default	0	0	96	0	0

Service	Forwarded Data(KB)	Dropped Data(KB)	Rejected Data(KB)	Matched Auto Connection	Matched Service Ports Connection
⊞aol-icq	0	0	0	0	0
⊞qq	0	0	0	0	0
⊞jabber	10	0	0	54	0
⊞odigo	0	0	0	0	0
⊞rediff	0	0	0	0	0
⊞eDonkey	0	0	0	0	0
⊞kad	0	0	0	0	0
⊞bittorrent	0	0	0	0	0
⊞ezpeer	0	0	0	0	0
⊞kuro	0	0	0	0	0
⊞gnutella	0	0	0	0	0
⊞fasttrack	0	0	0	0	0
⊞napster	0	0	0	0	0
⊞soulseek	0	0	0	0	0
⊞pp365	0	0	0	0	0
⊞poco	0	0	0	0	0
⊞qqlive	0	0	0	0	0
⊞pplive	0	0	0	0	0
⊞thunder	9	0	0	2	0
⊞http	3980192	0	0	55660	0
⊞ftp	10916123	0	0	292	0
⊞pop3	75267	0	0	2977	0

The following table describes the labels in this screen.

Table 119 AppPatrol > Statistics: Protocol Statistics

LABEL	DESCRIPTION
Service	This is the protocol. Click the expand icon (+) to display the statistics for each of a protocol's rules. Click the close icon (-) to hide the statistics for each of a protocol's rules.
Forwarded Data (KB)	This is how much of the application's traffic the ZyWALL has sent (in kilobytes).
Dropped Data (KB)	This is how much of the application's traffic the ZyWALL has discarded without notifying the client (in kilobytes). This traffic was dropped because it matched an application policy set to "drop".
Rejected Data (KB)	This is how much of the application's traffic the ZyWALL has discarded and notified the client that the traffic was rejected (in kilobytes). This traffic was rejected because it matched an application policy set to "reject".
Matched Auto Connection	This is how much of the application's traffic the ZyWALL identified by examining the IP payload.
Matched Service Ports Connection	This is how much of the application's traffic the ZyWALL identified by examining OSI level-3 information such as IP addresses and port numbers.
Rule	This is a protocol's rule.
Inbound Kbps	This is the incoming bandwidth usage for traffic that matched this protocol rule, in kilobits per second. This is the protocol's traffic that the ZyWALL sends to the initiator of the connection. So for a connection initiated from the LAN to the WAN, the traffic sent from the WAN to the LAN is the inbound traffic.
Outbound Kbps	This is the outgoing bandwidth usage for traffic that matched this protocol rule, in kilobits per second. This is the protocol's traffic that the ZyWALL sends out from the initiator of the connection. So for a connection initiated from the LAN to the WAN, the traffic sent from the LAN to the WAN is the outbound traffic.

Table 119 AppPatrol > Statistics: Protocol Statistics (continued)

LABEL	DESCRIPTION
Forwarded Data (KB)	This is how much of the application's traffic the ZyWALL has sent (in kilobytes).
Dropped Data (KB)	This is how much of the application's traffic the ZyWALL has discarded without notifying the client (in kilobytes). This traffic was dropped because it matched a policy set to "drop".
Rejected Data (KB)	This is how much of the application's traffic the ZyWALL has discarded and notified the client that the traffic was rejected (in kilobytes). This traffic was rejected because it matched a policy set to "reject".

28

Anti-Virus

This chapter introduces and shows you how to configure the anti-virus scanner. See Section 5.4.14 on page 120 for related information on these screens.

28.1 Anti-Virus Overview

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

28.1.1 Types of Computer Viruses

The following table describes some of the common computer viruses.

Table 120 Common Computer Virus Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable.
Macro Virus	Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network.
E-mail Virus	E-mail viruses are malicious programs that spread through e-mail.

28.1.2 Computer Virus Infection and Prevention

The following describes a simple life cycle of a computer virus.

1. A computer gets a copy of a virus from a source such as the Internet, e-mail, file sharing or any removable storage media. The virus is harmless until the execution of an infected program.
2. The virus spreads to other files and programs on the computer.
3. The infected files are unintentionally sent to another computer thus starting the spread of the virus.

4 Once the virus is spread through the network, the number of infected networked computers can grow exponentially.

28.1.3 Types of Anti-Virus Scanner

The section describes two types of anti-virus scanner: host-based and network-based.

A host-based anti-virus (HAV) scanner is often software installed on computers and/or servers in the network. It inspects files for virus patterns as they are moved in and out of the hard drive. However, host-based anti-virus scanners cannot eliminate all viruses for a number of reasons:

- HAV scanners are slow in stopping virus threats through real-time traffic (such as from the Internet).
- HAV scanners may reduce computing performance as they also share the resources (such as CPU time) on the computer for file inspection.
- You have to update the virus signatures and/or perform virus scans on all computers in the network regularly.

A network-based anti-virus (NAV) scanner is often deployed as a dedicated security device (such as your ZyWALL) on the network edge. NAV scanners inspect real-time data traffic (such as E-mail messages or web) that tends to bypass HAV scanners. The following lists some of the benefits of NAV scanners.

- NAV scanners stops virus threats at the network edge before they enter or exit a network.
- NAV scanners reduce computing loading on computers as the read-time data traffic inspection is done on a dedicated security device.

28.2 Introduction to the ZyWALL Anti-Virus Scanner

The ZyWALL has a built-in signature database. Setting up the ZyWALL between your local network and the Internet allows the ZyWALL to scan files transmitting through the enabled interfaces into your network. As a network-based anti-virus scanner, the ZyWALL helps stop threats at the network edge before they reach the local host computers.

You can set the ZyWALL to examine files received through the following protocols:

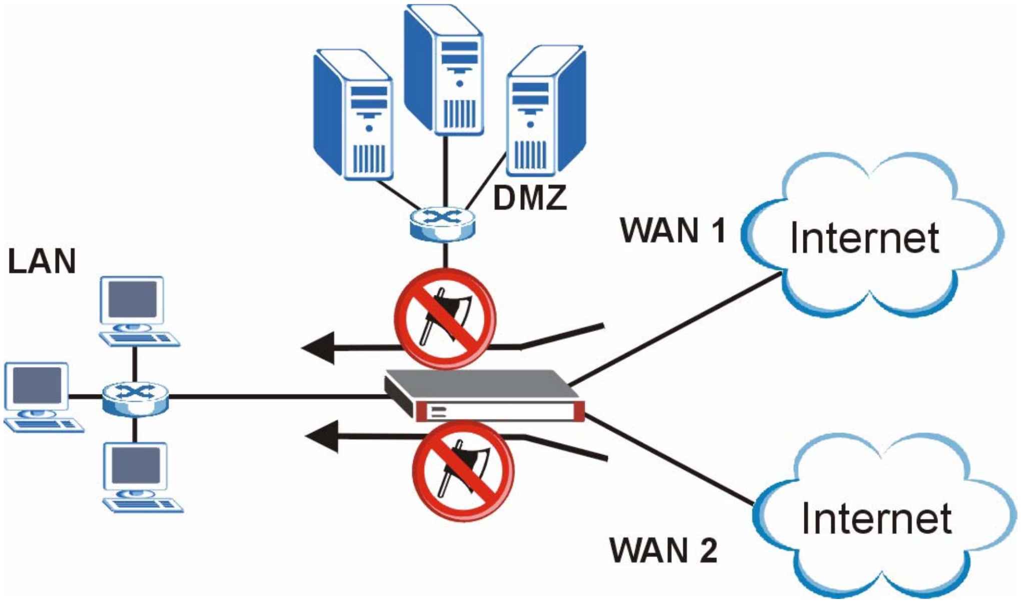
- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)
- IMAP4 (Internet Message Access Protocol version 4)

28.2.1 How the ZyWALL Anti-Virus Scanner Works

The ZyWALL checks traffic going in the direction(s) you specify for signature matches.

In the following figure the ZyWALL is set to check traffic coming from the WAN zone (which includes two interfaces) to the LAN zone.

Figure 313 ZyWALL Anti-virus Example



The following describes the virus scanning process on the ZyWALL.

1. The ZyWALL first identifies SMTP, POP3, IMAP4, HTTP and FTP packets through standard ports.
2. If the packets are not session connection setup packets (such as SYN, ACK and FIN), the ZyWALL records the sequence of the packets.
3. The scanning engine checks the contents of the packets for virus.
4. If a virus pattern is matched, the ZyWALL removes the infected portion of the file along with the rest of the file. The un-infected portion of the file before a virus pattern was matched still goes through.
5. If the send alert message function is enabled, the ZyWALL sends an alert to the file's intended destination computer(s).

Since the ZyWALL erases the infected portion of the file before sending it, you may not be able to open the file.

28.2.2 Notes About the ZyWALL Anti-Virus

The following lists important notes about the anti-virus scanner:

1. When a virus is detected, an alert message is displayed in Microsoft Windows computers.[4]
2. The ZyWALL does not scan the following file/traffic types:
   - Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.

---

[4] Refer to Appendix D on page 707 if your Windows computer does not display the alert messages.

- Encrypted traffic. This could be password-protected files or VPN traffic where the ZyWALL is not the endpoint (pass-through VPN traffic).
- Traffic through custom (non-standard) ports. The only exception is FTP traffic. The ZyWALL scans whatever port number is specified for FTP in the ALG screen.
- ZIP file(s) within a ZIP file.

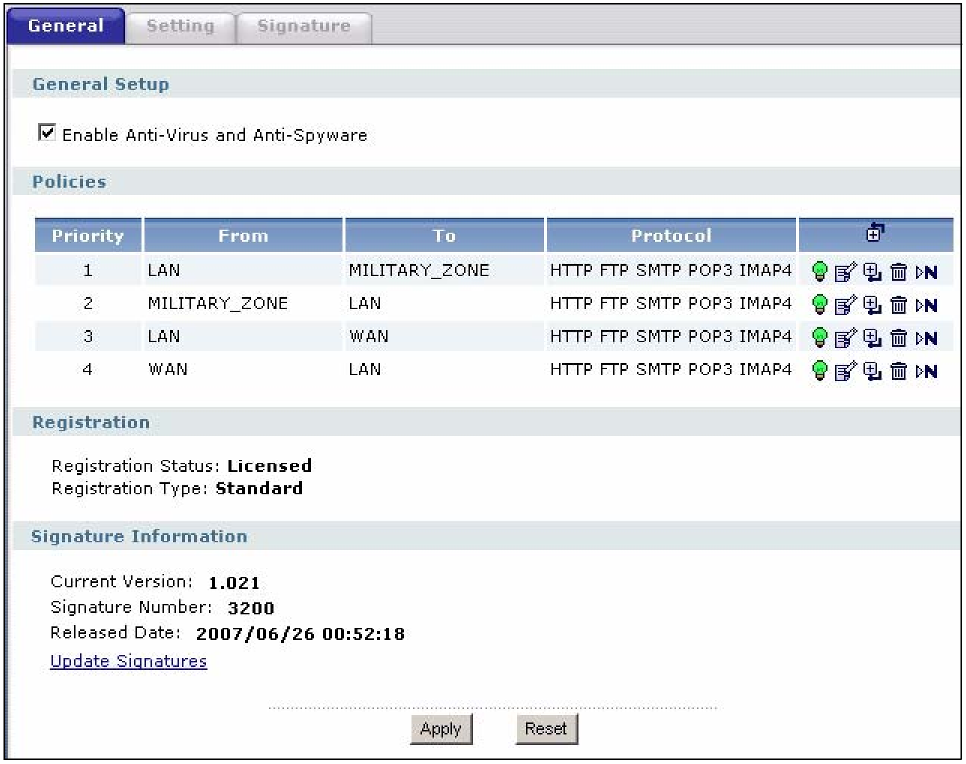
28.3 Anti-Virus Summary

Click **Anti-X** > **Anti-Virus** to display the configuration screen as shown next.

You must register for the anti-virus service (at least the trial) before you can use it.

See Chapter 8 on page 165 for how to register.

Figure 314 Anti-X > Anti-Virus > General



General Setup

☑ Enable Anti-Virus and Anti-Spyware

Policies

Priority	From	To	Protocol
1	LAN	MILITARY_ZONE	HTTP FTP SMTP POP3 IMAP4
2	MILITARY_ZONE	LAN	HTTP FTP SMTP POP3 IMAP4
3	LAN	WAN	HTTP FTP SMTP POP3 IMAP4
4	WAN	LAN	HTTP FTP SMTP POP3 IMAP4

Registration

Registration Status: **Licensed**
Registration Type: **Standard**

Signature Information

Current Version: **1.021**
Signature Number: **3200**
Released Date: **2007/06/26 00:52:18**
Update Signatures

The following table describes the labels in this screen.

Table 121 Anti-X > Anti-Virus > General

LABEL	DESCRIPTION
Enable Anti-Virus and Anti-Spyware	Select this check box to check traffic for viruses and spyware. The following table lists rules that define which traffic the ZyWALL scans and the action it takes upon finding a virus.
Priority	This is the position of an anti-virus rule in the list. The ordering of your anti-virus rules is important as the ZyWALL applies them in sequence. Once traffic matches an anti-virus rule, the ZyWALL applies that rule and does not check the traffic against any more rules.
From	The anti-virus rule has the ZyWALL scan traffic coming from this zone and going to the **To** zone.
To	The anti-virus rule has the ZyWALL scan traffic going to this zone from the **From** zone.
Protocol	These are the protocols of traffic to scan for viruses. **FTP** applies to traffic using the TCP port number specified for FTP in the ALG screen. **HTTP** applies to traffic using TCP ports 80, 8080 and 3128. **SMTP** applies to traffic using TCP port 25. **POP3** applies to traffic using TCP port 110. **IMAP4** applies to traffic using TCP port 143.
Add icon	Click the **Add** icon in the heading row to add a new first entry. The **Active** displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the entry on the ZyWALL. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action. In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the rule you are moving becomes number 6 and the previous rule 6 (if there is one) gets pushed up (or down) one. The ordering of your rules is important as they are applied in order of their numbering.
Registration	The following fields display information about the current state of your subscription for virus signatures.
Registration Status	This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**).
Registration Type	This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). **None** displays when the service is not activated.
Apply new Registration	This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service.
Signature Information	The following fields display information on the current signature set that the ZyWALL is using.
Current Version	This field displays the anti-virus signature set version number. This number gets larger as the set is enhanced.
Signature Number	This field displays the number of anti-virus signatures in this set.

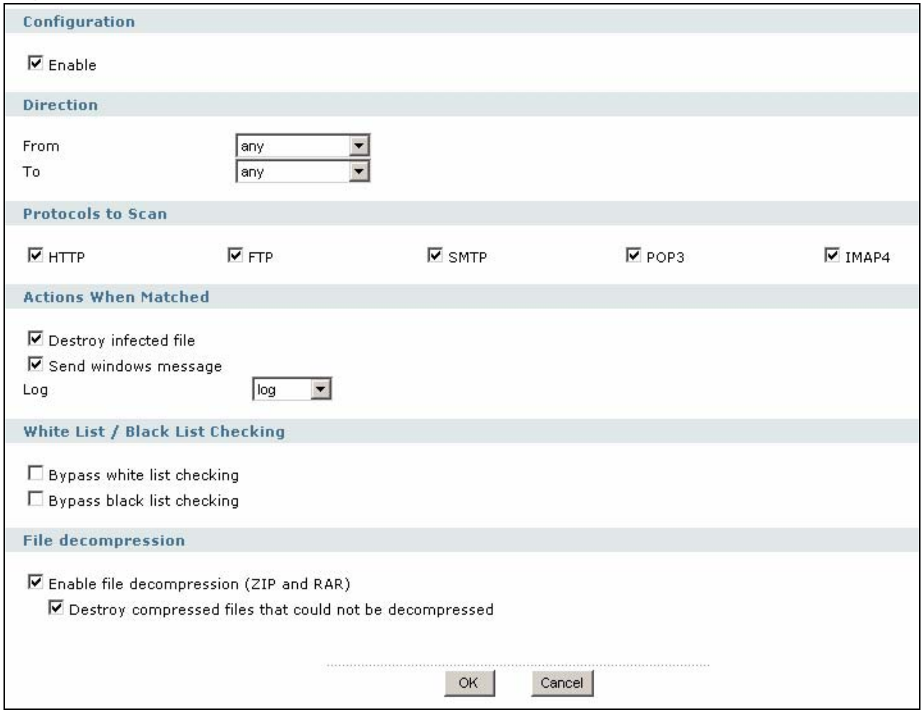
Table 121 Anti-X > Anti-Virus > General (continued)

LABEL	DESCRIPTION
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to start configuring this screen again.

28.3.1 Anti-Virus Policy Edit

Click the **Add** or **Edit** icon in the **Anti-X** > **Anti-Virus > General** screen to display the configuration screen as shown next.

Figure 315 Anti-X > Anti-Virus > General > Edit



Configuration

☑ Enable

Direction

From: any

To: any

Protocols to Scan

☑ HTTP ☑ FTP ☑ SMTP ☑ POP3 ☑ IMAP4

Actions When Matched

☑ Destroy infected file

☑ Send windows message

Log: log

White List / Black List Checking

☐ Bypass white list checking

☐ Bypass black list checking

File decompression

☑ Enable file decompression (ZIP and RAR)

☑ Destroy compressed files that could not be decompressed

The following table describes the labels in this screen.

Table 122 Anti-X > Anti-Virus > General > Edit

LABEL	DESCRIPTION
Enable	Select this check box to have the ZyWALL apply this anti-virus rule to check traffic for viruses.
From To	Select source and destination zones for traffic to scan for viruses. The anti-virus rule has the ZyWALL scan traffic coming from the **From** zone and going to the **To** zone.

Table 122 Anti-X > Anti-Virus > General > Edit (continued)

LABEL	DESCRIPTION
Protocols to Scan	Select which protocols of traffic to scan for viruses. **FTP** applies to traffic using the TCP port number specified for FTP in the ALG screen. **HTTP** applies to traffic using TCP ports 80, 8080 and 3128. **SMTP** applies to traffic using TCP port 25. **POP3** applies to traffic using TCP port 110. **IMAP4** applies to traffic using TCP port 143.
Actions When Matched	
Destroy infected file	When you select this check box, if a virus pattern is matched, the ZyWALL overwrites the infected portion of the file (and the rest of the file) with zeros. The un-infected portion of the file before a virus pattern was matched goes through unmodified.
Send Windows Message	Select this check box to set the ZyWALL to send a message alert to files' intended user(s) using Microsoft Windows computers connected to the to interface.
Log	These are the log options: **no**: Do not create a log when a packet matches a signature(s). **log**: Create a log on the ZyWALL when a packet matches a signature(s). **log alert**: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the ZyWALL send an alert when a packet matches a signature(s).
White List / Black List Checking	
Bypass white list checking	Select this check box to not check files against the white list. This disables the white list for traffic that matches this anti-virus rule.
Bypass black list checking	Select this check box to not check files against the black list. This disables the black list for traffic that matches this anti-virus rule.
File decompression	
Enable file decompression (ZIP and RAR)	Select this check box to have the ZyWALL scan a ZIP file (the file does not have to have a "zip" or "rar" file extension). The ZyWALL first decompresses the ZIP file and then scans the contents for viruses. Note: The ZyWALL decompresses a ZIP file once. The ZyWALL does NOT decompress any ZIP file(s) within a ZIP file.

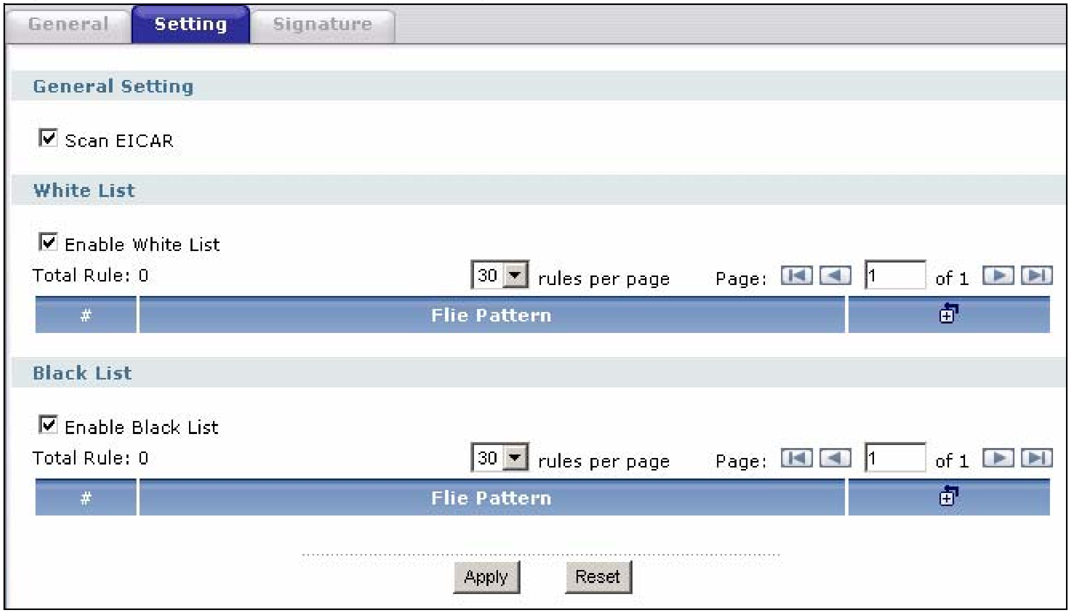
Table 122 Anti-X > Anti-Virus > General > Edit (continued)

LABEL	DESCRIPTION
Destroy compressed files that could not be decompressed	Note: When you select this option, the ZyWALL deletes ZIP files that use password encryption. Select this check box to have the ZyWALL delete any ZIP files that it is not able to unzip. The ZyWALL cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the ZyWALL can concurrently unzip. Note: The ZyWALL's firmware package cannot go through the ZyWALL with this option enabled. The ZyWALL classifies the firmware package as not being able to be decompressed and deletes it. You can upload the firmware package to the ZyWALL with the option enabled, so you only need to clear this option while you download the firmware package.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

28.4 Anti-Virus Setting

Click **Anti-X** > **Anti-Virus > Setting** screen to display the configuration screen as shown next.

Figure 316 Anti-X > Anti-Virus > Setting



General
Setting
Signature
General Setting
☑ Scan EICAR
White List
☑ Enable White List
Total Rule: 0
30 rules per page
Page: 1 of 1
#
Flie Pattern
Black List
☑ Enable Black List
Total Rule: 0
30 rules per page
Page: 1 of 1
#
Flie Pattern
Apply
Reset

The following table describes the labels in this screen.

Table 123 Anti-X > Anti-Virus > Setting

LABEL	DESCRIPTION
Scan EICAR	Select this option to have the ZyWALL check for the EICAR test file and treat it in the same way as a real virus file. The EICAR test file is a standardized test file for signature based anti-virus scanners. When the virus scanner detects the EICAR file, it responds in the same way as if it found a real virus. Besides straightforward detection, the EICAR file can also be compressed to test whether the anti-virus software can detect it in a compressed file. The test string consists of the following human-readable ASCII characters. X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
White List	Use the white list to have the ZyWALL not perform the anti-virus check on files with names that match the white list patterns.
Enable White List	Select this check box to have the ZyWALL not perform the anti-virus check on files with names that match the white list patterns.
Total Rule	This is the number of entries configured.
rules per page	Select how many entries you want to display on each page.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This is the entry's index number in the list.
File Pattern	This is the file name pattern. If a file's name matches this pattern, the ZyWALL does not check the file for viruses.
Add icon	This column provides icons to add, activate / deactivate, edit, and remove entries. To add an entry, click the **Add** icon at the top of the column. Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click an entry's **Edit** icon to edit the entry. To delete an entry, click the entry's **Remove** icon. The web configurator confirms that you want to delete the entry.
Black List	Use the black list to log and delete files with names that match the black list patterns.
Enable Black List	Select this check box to log and delete files with names that match the black list patterns.
Total Rule	This is the number of entries configured.
rules per page	Select how many entries you want to display on each page.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This is the entry's index number in the list.
File Pattern	This is the file name pattern. If a file's name that matches this pattern, the ZyWALL logs and deletes the file.
Add icon	This column provides icons to add, activate / deactivate, edit, and remove entries. To add an entry, click the **Add** icon at the top of the column. Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click an entry's **Edit** icon to edit the entry. To delete an entry, click the entry's **Remove** icon. The web configurator confirms that you want to delete the entry.

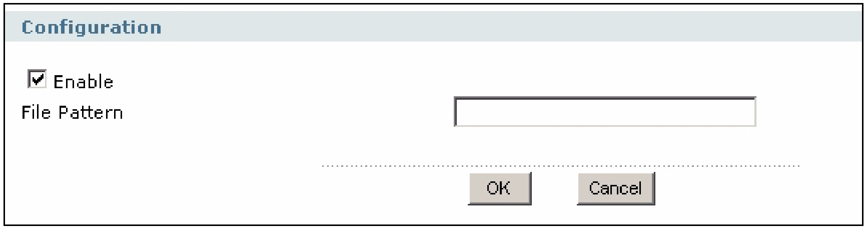
Table 123 Anti-X > Anti-Virus > Setting (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to start configuring this screen again.

28.5 Anti-Virus White List Add/Edit

From the **Anti-X** > **Anti-Virus > Setting** screen, click a white list **Add** icon or **Edit** icon to display the following screen. Use this screen to create an anti-virus white list entry for a file pattern that should cause the ZyWALL to not scan a file for viruses.

Figure 317 Anti-X > Anti-Virus > Setting > White List Add



The following table describes the labels in this screen.

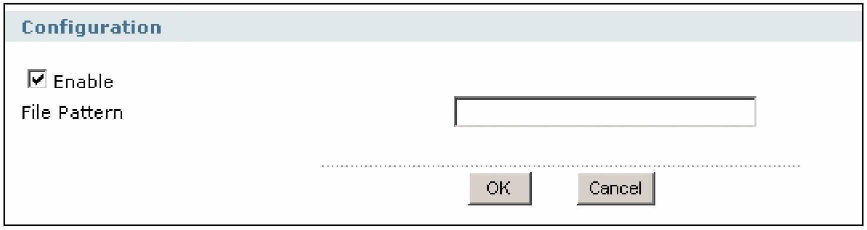
Table 124 Anti-X > Anti-Virus > Setting > White List Add

LABEL	DESCRIPTION
Enable	Select this option to have the ZyWALL apply this white list entry when using the white list.
File Pattern	Specify a pattern to identify the names of files that the ZyWALL should not scan for viruses. Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. A * in the middle of a pattern has the ZyWALL check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the ZyWALL checks up to the first 80 characters of a file name.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

28.6 Anti-Virus Black List Add/Edit

From the **Anti-X** > **Anti-Virus > Setting** screen, click a black list **Add** icon or **Edit** icon to display the following screen. Use this screen to create an anti-virus black list entry for a file pattern that should cause the ZyWALL to log and delete a file.

Figure 318 Anti-X > Anti-Virus > Setting > Black List Add



The following table describes the labels in this screen.

Table 125 Anti-X > Anti-Virus > Setting > Black List Add

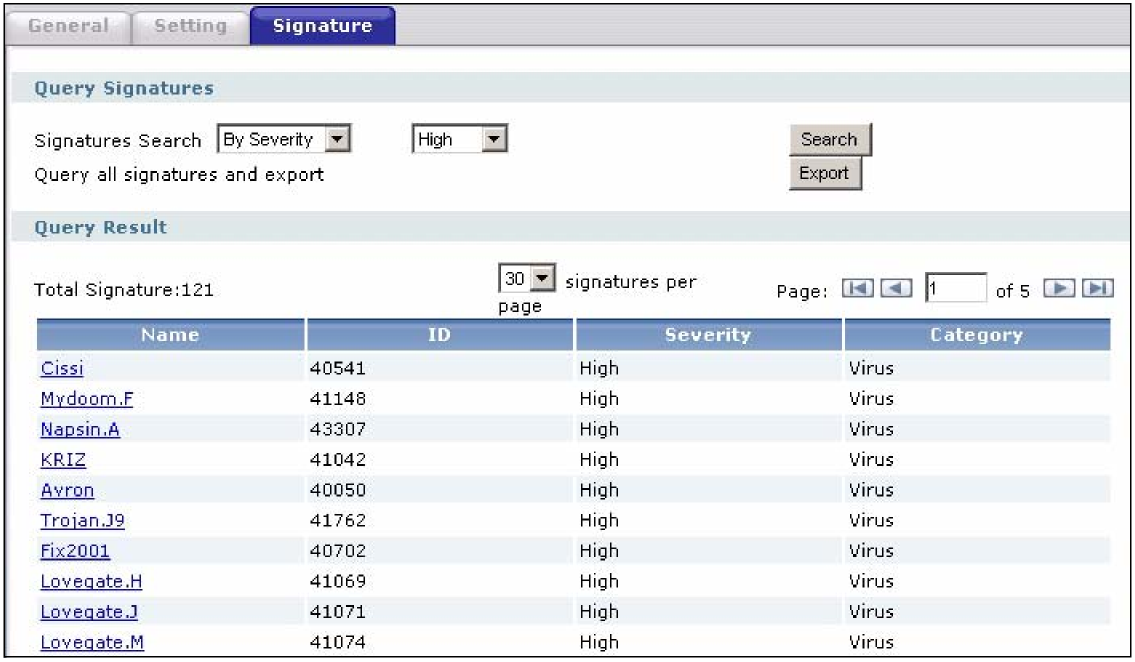
LABEL	DESCRIPTION
Enable	Select this option to have the ZyWALL apply this black list entry when using the black list.
File Pattern	Specify a pattern to identify the names of files that the ZyWALL should log and delete. Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. A * in the middle of a pattern has the ZyWALL check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the ZyWALL checks up to the first 80 characters of a file name.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

28.7 Signature Searching

Click **Anti-X** > **Anti-Virus > Signature** to display this screen. Use this screen to locate signatures and display details about them.

If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

Figure 319 Anti-X > Anti-Virus > Signature: Search by Severity



Signatures Search By Severity High

Query all signatures and export

Total Signature:121

30 signatures per page

Page: 1 of 5

Name	ID	Severity	Category
Cissi	40541	High	Virus
Mydoom.F	41148	High	Virus
Napsin.A	43307	High	Virus
KRIZ	41042	High	Virus
Avron	40050	High	Virus
Trojan.J9	41762	High	Virus
Fix2001	40702	High	Virus
Lovegate.H	41069	High	Virus
Lovegate.J	41071	High	Virus
Lovegate.M	41074	High	Virus

The following table describes the labels in this screen.

Table 126 Anti-X > Anti-Virus > Signature

LABEL	DESCRIPTION
Signatures Search	Select the criteria on which to perform the search. Select **By Name** from the drop down list box and type the name or part of the name of the signature(s) you want to find. This search is not case-sensitive. Select **By ID** from the drop down list box and type the ID or part of the ID of the signature you want to find. Select **By Severity** from the drop down list box and select the severity level of the signatures you want to find. Select **By Category** from the drop down list box and select whether you want to see virus signatures or spyware signatures. Click **Search** to have the ZyWALL search the signatures based on your specified criteria.
Query Signatures and Export	Click **Export** to have the ZyWALL save all of the anti-virus signatures to your computer in a .txt file.
Query Result	
Total Signature	This is the number of signatures that matched your search criteria.
signatures per page	Select how many entries you want to display on each page.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
Name	This is the name of the anti-virus signature. Click the **Name** column heading to sort your search results in ascending or descending order according to the signature name. Click a signature's name to see details about the virus.
ID	This is the IDentification number of the anti-virus signature. Click the ID column header to sort your search results in ascending or descending order according to the ID.

Table 126 Anti-X > Anti-Virus > Signature (continued)

LABEL	DESCRIPTION
Severity	This is the severity level of the anti-virus signature. Click the severity column header to sort your search results by ascending or descending severity.
Category	This column displays whether the signature is for identifying a virus or spyware. Click the column heading to sort your search results by category.

29

IDP

This chapter introduces IDP (Intrusion, Detection and Prevention), IDP profiles, binding an IDP profile to a traffic direction, custom signatures and updating signatures. See Section 5.4.15 on page 120 for related information on these screens.

29.1 Introduction to IDP

An IDP system can detect malicious or suspicious packets and respond instantaneously. It is designed to detect pattern-based attacks.

29.1.1 Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install a host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

29.1.2 Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda MyDoom etc.

29.1.3 IDP on the ZyWALL

IDP on the ZyWALL protects against network-based intrusions. See Section 29.8.2 on page 427 for a list of attacks that the ZyWALL can protect against. You can also create your own custom IDP rules.

29.1.4 Signatures

If a packet matches a signature, the action specified by the signature is taken. You can change the default signature actions in the profile screens.

29.2 Traffic Directions and Profiles

A zone is a combination of ZyWALL interfaces and VPN connections for security. See the zone chapter for details on zones and the interfaces chapter for details on interfaces. Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to.

An IDP profile is a set of IDP rules with configured activation, log and action settings. The ZyWALL comes with default profiles that you can bind to traffic directions. For example, by default, the default LAN_IDP profile is bound to any traffic going to the LAN zone. You could use this to protect your LAN computers.

You can also create your own IDP profiles from base profiles. See Table 129 on page 422 for details on base profiles.

You can only bind one profile to one traffic direction.

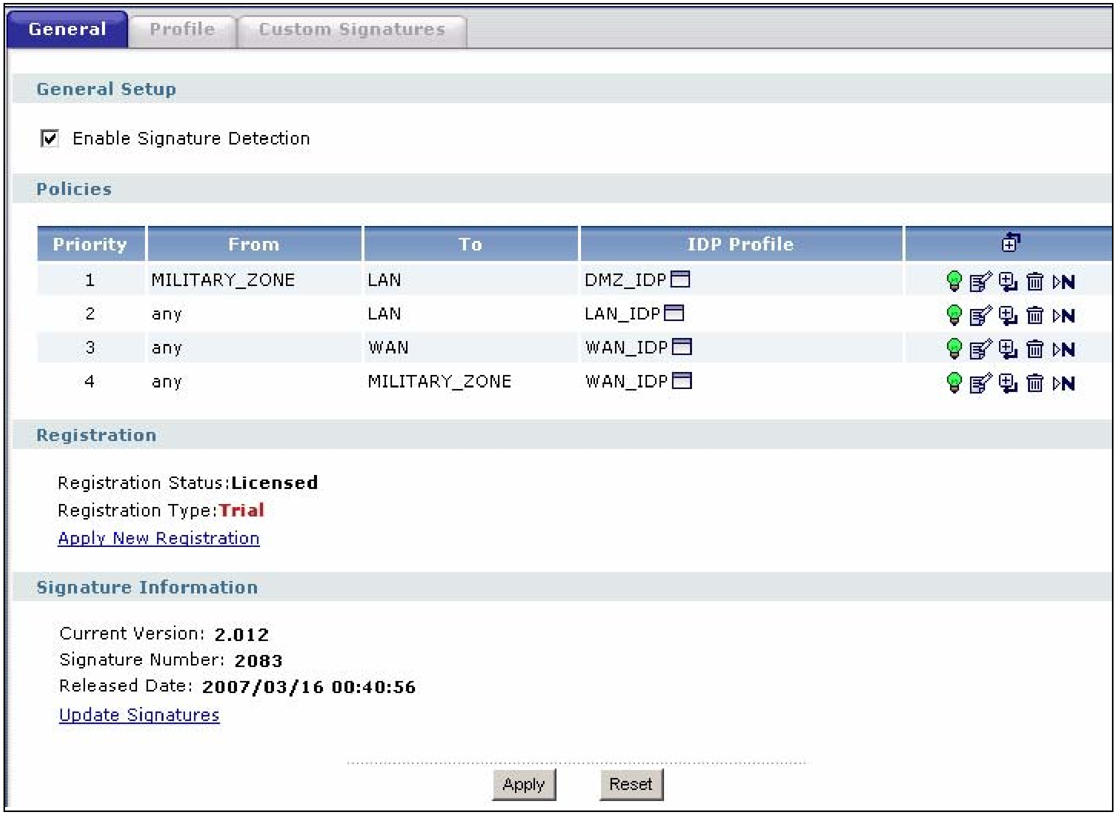
29.3 Configuring IDP General

Click **Anti-X** > **IDP** > **General** to open this screen. Use this screen to turn IDP on or off, bind IDP profiles to traffic directions, and view registration and signature information.

You must register in order to use packet inspection signatures. See the **Registration** screens.

If you try to enable IDP when the IDP service has not yet been registered, a warning screen displays and IDP is not enabled.

Figure 320 Anti-X > IDP > General



General Setup

☑ Enable Signature Detection

Policies

Priority	From	To	IDP Profile	
1	MILITARY_ZONE	LAN	DMZ_IDP	
2	any	LAN	LAN_IDP	
3	any	WAN	WAN_IDP	
4	any	MILITARY_ZONE	WAN_IDP	

Registration

Registration Status:**Licensed**
Registration Type:**Trial**
Apply New Registration

Signature Information

Current Version: **2.012**
Signature Number: **2083**
Released Date: **2007/03/16 00:40:56**
Update Signatures

The following table describes the screens in this screen.

Table 127 Anti-X > IDP > General

LABEL	DESCRIPTION
General Setup	
Enable Signature Detection	You must register for IDP service in order to use packet inspection signatures. If you don't have a standard license, you can register for a once-off trial one.
Bindings	Use this list to specify which IDP profile the ZyWALL uses for traffic flowing in a specific direction.
Priority	This is this binding's rank in the list of IDP profile to traffic direction bindings. The list is applied in order of priority.
From, To	This is the direction of travel of packets to which an IDP profile is bound. Note: Depending on your network topology and traffic load, binding every packet direction to an IDP profile may affect the ZyWALL's performance. **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet via the ZyWALL's LAN zone interfaces. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet. **From WAN To WAN** means packets that come in from the WAN zone and the ZyWALL routes back out through the WAN zone.
IDP Profile	An IDP profile is a set of IDP rules with configured activation, log and action settings. This field shows which IDP profile is bound to which traffic direction. Click the **popup** icon to change to a different profile.

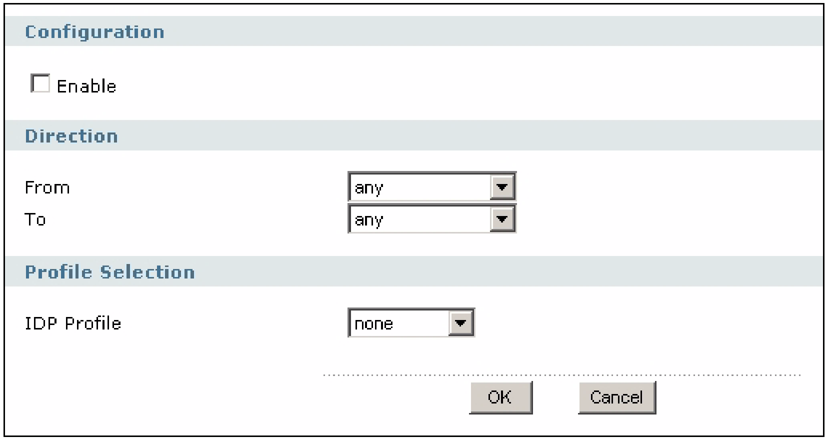
Table 127 Anti-X > IDP > General (continued)

LABEL	DESCRIPTION
(Icons)	Click the **Add** icon in the heading row to add a new first entry. The **Active** icon displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Add** icon in an entry to add an entry below the current entry. Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action. In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one. The ordering of your entries is important as they are applied in order of their numbering.
Registration	You need to create an account at myZyXEL.com, register your ZyWALL and then subscribe for IDP in order to be able to download new packet inspection signatures from myZyXEL.com. There's an initial free trial period for IDP after which you must pay to subscribe to the service. See the Registration chapter for details.
Registration Status	**Licensed**, **Not Licensed** or **Expired** indicates whether you have subscribed for IDP services or not or your registration has expired.
Registration Type	This field shows **Trial**, **Standard** or **None** depending on whether you subscribed to the IDP trial, bought an iCard for IDP service or neither.
Apply new Registration	This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service.
Signature Information	The following fields display information on the current signature set that the ZyWALL is using.
Current Version	This field displays the IDP signature set version number. This number gets larger as the set is enhanced.
Signature Number	This field displays the number of IDP signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to start configuring this screen again.

29.4 Configuring IDP Bindings

Click **Anti-X > IDP > General** and then an **Add** or **Edit** icon to display the following screen. Use this screen to bind an IDP profile to a traffic direction.

Figure 321 Anti-X > IDP > General > Add



The following table describes the screens in this screen.

Table 128 Anti-X > IDP > General > Add

LABEL	DESCRIPTION
Enable	Select this check box to turn on this IDP profile to traffic direction binding.
From	Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to. Use the **From** field to specify the zone from which the traffic is coming.
To	Use the **To** field to specify the zone to which the traffic is going.
IDP Profile	An IDP profile is a set of IDP rules with configured activation, log and action settings. Select an IDP profile to bind to the entry's traffic direction. Configure the IDP profiles in the IDP profile screens.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

29.5 Introducing IDP Profiles

An IDP profile is a set of packet inspection signatures.

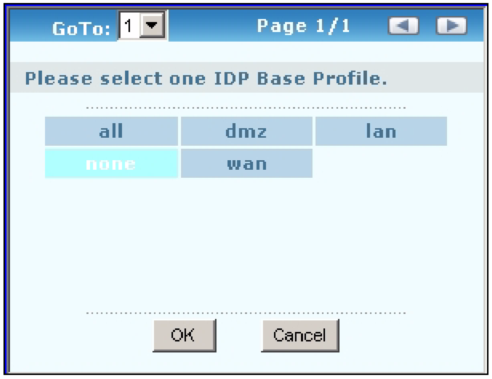
Packet inspection signatures examine packet content for malicious data. Packet inspection applies to OSI (Open System Interconnection) layer-4 to layer-7 contents. You need to subscribe for IDP service in order to be able to download new signatures.

In general, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior (see Chapter 30 on page 445 for information on anomaly detection).

29.5.1 Base Profiles

The ZyWALL comes with several base profiles. You use base profiles to create new profiles. In the **Anti-X** > **IDP** > **Profile** screen, click the **Add** icon to display the following screen.

Figure 322 Base Profiles



The following table describes this screen.

Table 129 Base Profiles

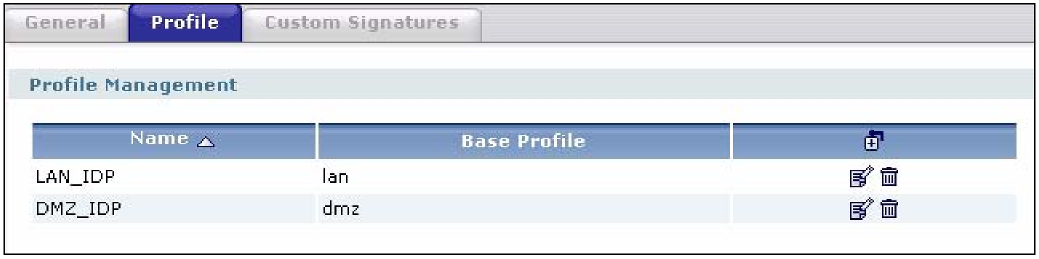
BASE PROFILE	DESCRIPTION
all	All signatures are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a very low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them.
dmz	This profile is most suitable for networks containing your servers. Signatures for common services such as DNS, FTP, HTTP, ICMP, IMAP, MISC, NETBIOS, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, Oracle, MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled.
lan	This profile is most suitable for common LAN network services. Signatures for common services such as DNS, FTP, HTTP, ICMP, IM, IMAP, MISC, NETBIOS, P2P, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, TFTP, MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate logs (not log alerts) and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled.
none	All signatures are disabled. No logs are generated nor actions are taken.
wan	Signatures for all services are enabled. Signatures with a medium, high or severe severity level (greater than two) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low or low severity level (less than or equal to two) are disabled.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

29.6 Profile Summary Screen

Select **Anti-X** > **IDP** > **Profile**. Use this screen to:

- Add a new profile
- Edit an existing profile
- Delete an existing profile

Figure 323 Anti-X > IDP > Profile



Name	Base Profile	
LAN_IDP	lan	
DMZ_IDP	dmz	

The following table describes the fields in this screen.

Table 130 Anti-X > IDP > Profile

LABEL	DESCRIPTION
Name	This is the name of the profile you created.
Base Profile	This is the base profile from which the profile was created.
(Icons)	Click the **Add** icon in the column header to create a new profile. A pop-up screen displays requiring you to choose a base profile from which to create the new profile. Click an **Edit** icon to edit an existing profile. Click a **Remove** icon to delete an existing profile.

29.7 Creating New Profiles

You may want to create a new profile if not all signatures in a base profile are applicable to your network. In this case you should disable non-applicable signatures so as to improve ZyWALL IDP processing efficiency.

You may also find that certain signatures are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL. As each network is different, false positives and false negatives are common on initial IDP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a signature.

29.7.1 Procedure To Create a New Profile

To create a new profile:

1 Click the **Add** icon in the **Anti-X** > **IDP** > **Profile** screen to display a pop-up screen allowing you to choose a base profile.

2 Select a base profile (see Table 129 on page 422) and then click **OK** to go to the profile details screen.

If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

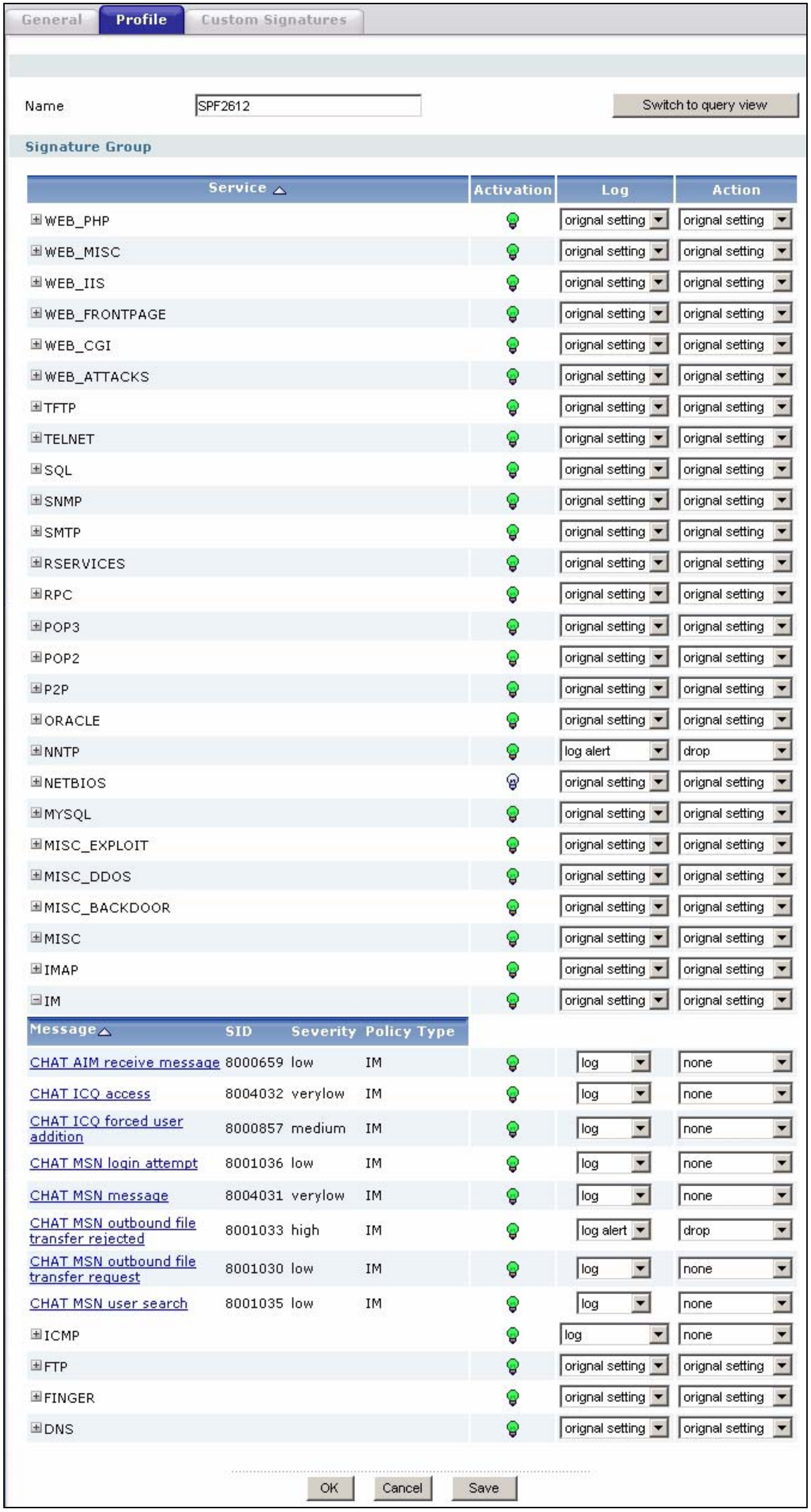
3 Type a new profile name
4 Enable or disable individual signatures.
5 Edit the default log options and actions.

29.8 Profiles: Packet Inspection

Select **Anti-X > IDP > Profile** and then add a new or edit an existing profile select. Packet inspection signatures examine the contents of a packet for malicious data. It operates at layer-4 to layer-7.

29.8.1 Profile > Group View Screen

Figure 324 Anti-X > IDP > Profile > Edit : Group View



Name: SPF2612

Signature Group

Service	Activation	Log	Action
⊞WEB_PHP	●	orignal setting	orignal setting
⊞WEB_MISC	●	orignal setting	orignal setting
⊞WEB_IIS	●	orignal setting	orignal setting
⊞WEB_FRONTPAGE	●	orignal setting	orignal setting
⊞WEB_CGI	●	orignal setting	orignal setting
⊞WEB_ATTACKS	●	orignal setting	orignal setting
⊞TFTP	●	orignal setting	orignal setting
⊞TELNET	●	orignal setting	orignal setting
⊞SQL	●	orignal setting	orignal setting
⊞SNMP	●	orignal setting	orignal setting
⊞SMTP	●	orignal setting	orignal setting
⊞RSERVICES	●	orignal setting	orignal setting
⊞RPC	●	orignal setting	orignal setting
⊞POP3	●	orignal setting	orignal setting
⊞POP2	●	orignal setting	orignal setting
⊞P2P	●	orignal setting	orignal setting
⊞ORACLE	●	orignal setting	orignal setting
⊞NNTP	●	log alert	drop
⊞NETBIOS	○	orignal setting	orignal setting
⊞MYSQL	●	orignal setting	orignal setting
⊞MISC_EXPLOIT	●	orignal setting	orignal setting
⊞MISC_DDOS	●	orignal setting	orignal setting
⊞MISC_BACKDOOR	●	orignal setting	orignal setting
⊞MISC	●	orignal setting	orignal setting
⊞IMAP	●	orignal setting	orignal setting
⊟IM	●	orignal setting	orignal setting

Message	SID	Severity	Policy Type			
CHAT AIM receive message	8000659	low	IM	●	log	none
CHAT ICQ access	8004032	verylow	IM	●	log	none
CHAT ICQ forced user addition	8000857	medium	IM	●	log	none
CHAT MSN login attempt	8001036	low	IM	●	log	none
CHAT MSN message	8004031	verylow	IM	●	log	none
CHAT MSN outbound file transfer rejected	8001033	high	IM	●	log alert	drop
CHAT MSN outbound file transfer request	8001030	low	IM	●	log	none
CHAT MSN user search	8001035	low	IM	●	log	none

⊞ICMP	●	log	none
⊞FTP	●	orignal setting	orignal setting
⊞FINGER	●	orignal setting	orignal setting
⊞DNS	●	orignal setting	orignal setting

The following table describes the fields in this screen.

Table 131 Anti-X > IDP > Profile > Group View

LABEL	DESCRIPTION
Name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: MyProfile mYProfile Mymy12_3-4 These are invalid profile names: 1mYProfile My Profile MyProfile? Whatalongprofilename123456789012
Switch to query view	Click this button to go to a screen where you can search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, service category, log options or actions.
Service	Click the + sign next to a service group to expand it. A service group is a group of related IDP signatures.
Message	This is the name of the signature.
SID	This is the signature ID (identification) number that uniquely identifies a ZyWALL signature.
Severity	These are the severities as defined in the ZyWALL. The number in brackets is the number you use if using commands. **Severe** (5): These denote attacks that try to run arbitrary code or gain system privileges. **High** (4): These denote known serious vulnerabilities or attacks that are probably not false alarms. **Medium** (3): These denote medium threats, access control attacks or attacks that could be false alarms. **Low** (2): These denote mild threats or attacks that could be false alarms. **Very Low** (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries etc.
Policy Type	This is the attack type as defined on the ZyWALL. See Table 132 on page 427 for a description of each type.
Activation	Click the icon to enable or disable a signature or group of signatures.
Log	These are the log options: **original setting**: Select this option to return each log option within a service group to its previously saved configuration. **no**: Select this option on an individual signature or a complete service group to have the ZyWALL create no log when a packet matches a signature(s). **log**: Select this option on an individual signature or a complete service group to have the ZyWALL create a log when a packet matches a signature(s). **log alert**: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the ZyWALL send an alert when a packet matches a signature(s).

Table 131 Anti-X > IDP > Profile > Group View (continued)

LABEL	DESCRIPTION
Action	Select what action the ZyWALL should take when a packet matches a signature here. **original setting**: Select this action to return each signature in a service group to its previously saved configuration. **none**: Select this action on an individual signature or a complete service group to have the ZyWALL take no action when a packet matches the signature(s). **drop**: Select this action on an individual signature or a complete service group to have the ZyWALL silently drop a packet that matches the signature(s). Neither sender nor receiver are notified. **reject-sender**: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to the sender when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with a 'RST' flag. If it is an ICMP or UDP attack packet, the ZyWALL will send an ICMP unreachable packet. **reject-receiver**: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to the receiver when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with an a 'RST' flag. If it is an ICMP or UDP attack packet, the ZyWALL will do nothing. **reject-both**: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to both the sender and receiver when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with a 'RST' flag to the receiver and sender. If it is an ICMP or UDP attack packet, the ZyWALL will send an ICMP unreachable packet.
OK	A profile consists of three separate screens. If you want to configure just one screen for an IDP profile, click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	If you want to configure more than one screen for an IDP profile, click **Save** to save the configuration to the ZyWALL, but remain in the same page. You may then go to another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

29.8.2 Policy Types

This section describes IDP policy types, also known as attack types, as categorized in the ZyWALL. You may refer to these types when categorizing your own custom rules.

Table 132 Policy Types

POLICY TYPE	DESCRIPTION
P2P	Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the ZyWALL, P2P refers to peer-to-peer applications such as e-Mule, e-Donkey, BitTorrent, iMesh, etc.
IM	IM (Instant Messaging) refers to chat applications. Chat is real-time, text-based communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any room member can type a message that will appear on the monitors of all the other participants.
SPAM	Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services.

Table 132 Policy Types (continued)

POLICY TYPE	DESCRIPTION
DoS/DDoS	The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
Scan	A scan describes the action of searching a network for an exposed service. An attack may then occur once a vulnerability has been found. Scans occur on several network levels. A network scan occurs at layer-3. For example, an attacker looks for network devices such as a router or server running in an IP network. A scan on a protocol is commonly referred to as a layer-4 scan. For example, once an attacker has found a live end system, he looks for open ports. A scan on a service is commonly referred to a layer-7 scan. For example, once an attacker has found an open port, say port 80 on a server, he determines that it is a HTTP service run by some web server application. He then uses a web vulnerability scanner (for example, Nikto) to look for documented vulnerabilities.
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.
Virus/Worm	A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm’s uncontrolled replication consumes system resources, thus slowing or stopping other tasks.
Backdoor/Trojan	A backdoor (also called a trapdoor) is hidden software or a hardware mechanism that can be triggered to gain access to a program, online service or an entire computer system. A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data. Although a virus, a worm and a Trojan are different types of attacks, they can be blended into one attack. For example, W32/Blaster and W32/Sasser are blended attacks that feature a combination of a worm and a Trojan.
Access Control	Access control refers to procedures and controls that limit or detect access. Access control attacks try to bypass validation checks in order to access network resources such as servers, directories, and files.
Web Attack	Web attacks refer to attacks on web servers such as IIS (Internet Information Services).

29.8.3 IDP Service Groups

An IDP service group is a set of related packet inspection signatures.

Table 133 IDP Service Groups

WEB_PHP	WEB_MISC	WEB_IIS	WEB_FRONTPAGE
WEB_CGI	WEB_ATTACKS	TFTP	TELNET
SQL	SNMP	SMTP	RSERVICES
RPC	POP3	POP2	P2P
ORACLE	NNTP	NETBIOS	MYSQL
MISC_EXPLOIT	MISC_DDOS	MISC_BACKDOOR	MISC

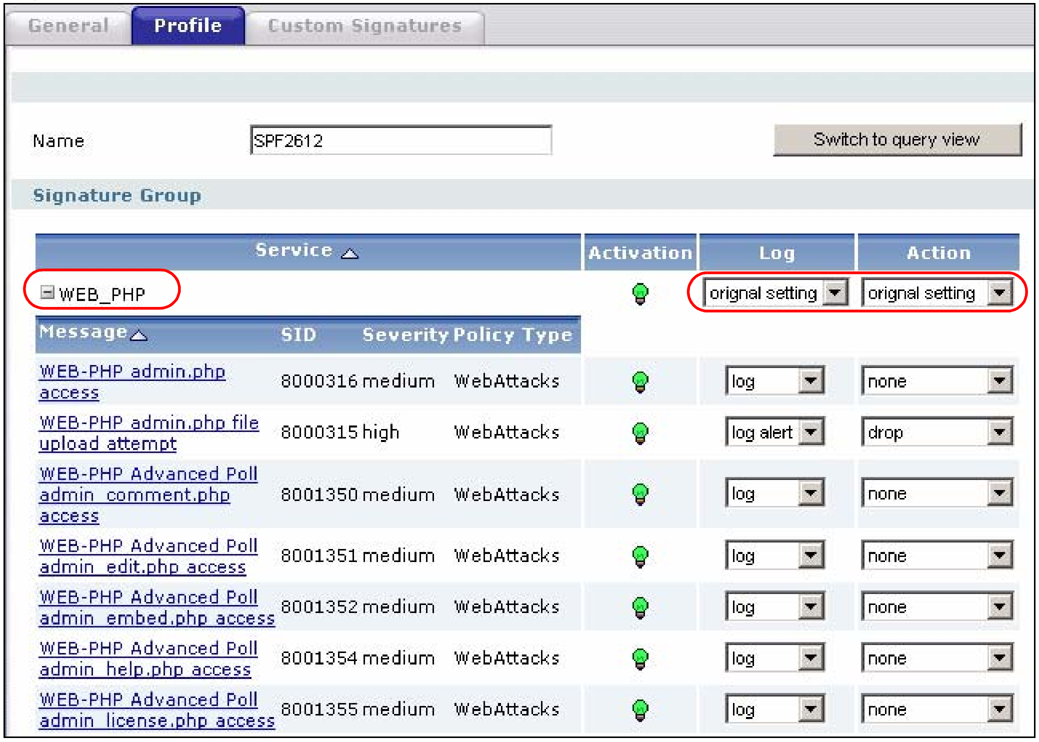
Table 133 IDP Service Groups (continued)

IMAP	IM	ICMP	FTP
FINGER	DNS		

The following figure shows the WEB_PHP service group that contains signatures related to attacks on web servers using PHP exploits. PHP (PHP: Hypertext Preprocessor) is a server-side HTML embedded scripting language that allows web developers to build dynamic websites.

Logs and actions applied to a service group apply to all signatures within that group. If you select **original setting** for service group logs and/or actions, all signatures within that group are returned to their last-saved settings.

Figure 325 Anti-X > IDP > Profile > Edit > IDP Service Group



Name: SPF2612

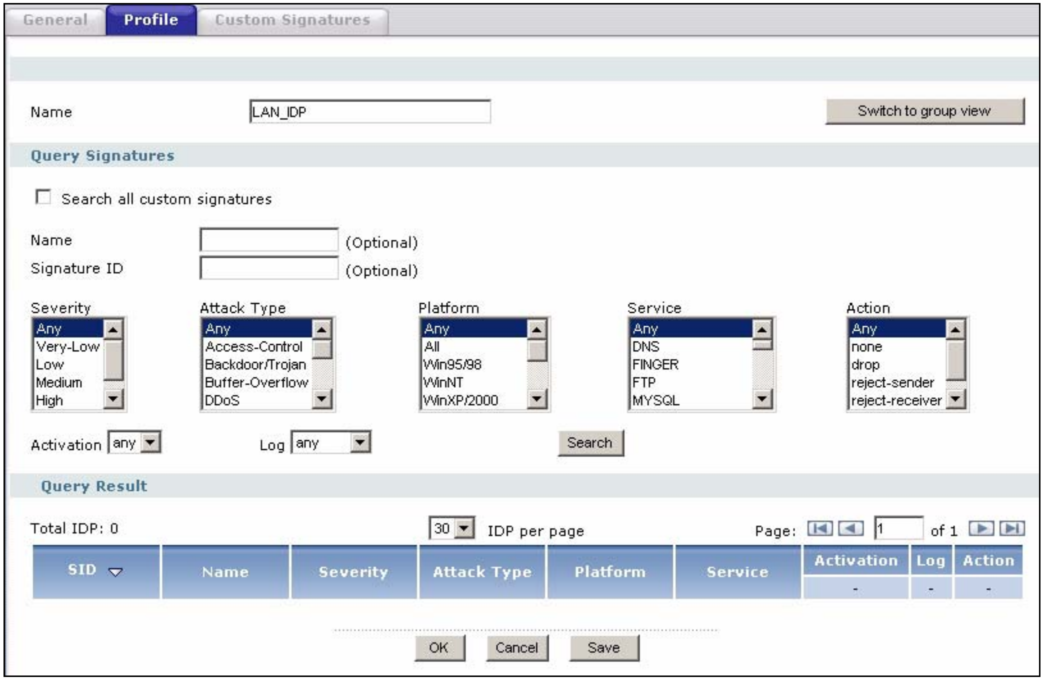
Service	Activation	Log	Action
⊟ WEB_PHP	●	orignal setting	orignal setting

Message	SID	Severity	Policy Type	Activation	Log	Action
WEB-PHP admin.php access	8000316	medium	WebAttacks	●	log	none
WEB-PHP admin.php file upload attempt	8000315	high	WebAttacks	●	log alert	drop
WEB-PHP Advanced Poll admin_comment.php access	8001350	medium	WebAttacks	●	log	none
WEB-PHP Advanced Poll admin_edit.php access	8001351	medium	WebAttacks	●	log	none
WEB-PHP Advanced Poll admin_embed.php access	8001352	medium	WebAttacks	●	log	none
WEB-PHP Advanced Poll admin_help.php access	8001354	medium	WebAttacks	●	log	none
WEB-PHP Advanced Poll admin_license.php access	8001355	medium	WebAttacks	●	log	none

29.8.4 Profile > Query View Screen

Click **Switch to query view** in the screen as shown in Figure 324 on page 425 to go to a signature query screen. In the query view screen, you can search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, service category, log options or actions.

Figure 326 Anti-X > IDP > Profile: Query View


General
Profile
Custom Signatures
Switch to group view
Query Signatures
☐ Search all custom signatures
(Optional)
(Optional)
Severity
Any
Very-Low
Low
Medium
High
Attack Type
Any
Access-Control
Backdoor/Trojan
Buffer-Overflow
DDoS
Platform
Any
All
Win95/98
WinNT
WinXP/2000
Service
Any
DNS
FINGER
FTP
MYSQL
Action
Any
none
drop
reject-sender
reject-receiver
Search
Query Result
SID
Name
Severity
Attack Type
Platform
Service
Activation
Log
Action
OK
Cancel
Save

Name: LAN_IDP

Name:

Signature ID:

Activation: any

Log: any

Total IDP: 0

30 IDP per page

Page: 1 of 1

Activation	Log	Action
-	-	-

The following table describes the fields in this screen.

Table 134 Anti-X > IDP > Profile: Query View

LABEL	DESCRIPTION
Name	This is the name of the profile that you created in the **IDP > Profiles > Group View** screen.
Switch to group view	Click this button to go to the IDP profile group view screen where IDP signatures are grouped by service and you can configure activation, logs and/or actions.
Query Signatures	Select the criteria on which to perform the search.
Search all custom signatures	Select this check box to search for signatures you created or imported in the **Custom Signatures** screen. You can search by name or ID. If the name and ID fields are left blank, then all custom signatures are displayed.
Name	Type the name or part of the name of the signature(s) you want to find.
Signature ID	Type the ID or part of the ID of the signature(s) you want to find.
Severity	Search for signatures by severity level(s) (see Table 131 on page 426). Hold down the [Ctrl] key if you want to make multiple selections.
Attack Type	Search for signatures by attack type(s) (see Table 132 on page 427). Attack types are known as policy types in the group view screen. Hold down the [Ctrl] key if you want to make multiple selections.
Platform	Search for signatures created to prevent intrusions targeting specific operating system(s). Hold down the [Ctrl] key if you want to make multiple selections.
Service	Search for signatures by IDP service group(s). See Table 133 on page 428 for group details. Hold down the [Ctrl] key if you want to make multiple selections.
Action	Search for signatures by the response the ZyWALL takes when a packet matches a signature. See Table 131 on page 426 for action details. Hold down the [Ctrl] key if you want to make multiple selections.
Activation	Search for enabled and/or disabled signatures here.
Log	Search for signatures by log option here. See Table 131 on page 426 for option details.

Table 134 Anti-X > IDP > Profile: Query View (continued)

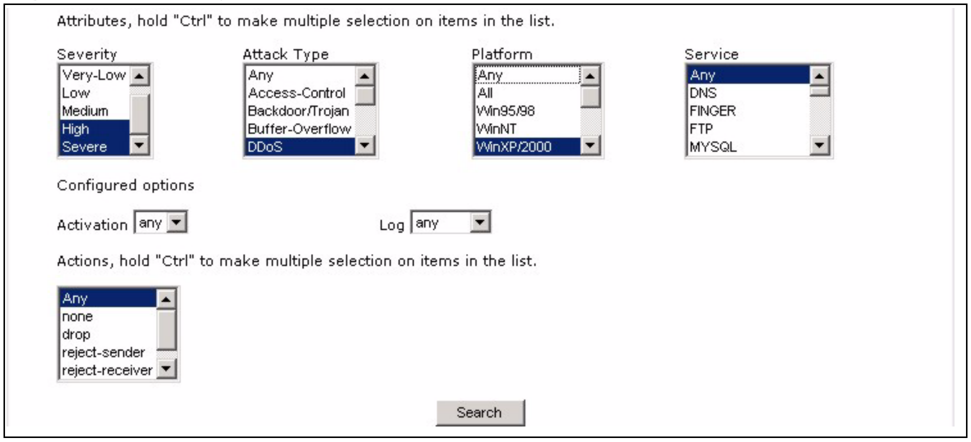
LABEL	DESCRIPTION
Search	Click this button to begin the search. The results display at the bottom of the screen. Results may be spread over several pages depending on how broad the search criteria selected were. The tighter the criteria selected, the fewer the signatures returned.
Query Result	The results are displayed in a table showing the **SID, Name, Severity, Attack Type, Platform, Service, Activation, Log**, and **Action** criteria as selected in the search. Click the **SID** column header to sort search results by signature ID.
Total IDP:	This displays the total number of signatures found in your search.
IDP per page	Select the number of signatures you want to appear per page here.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
OK	Click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the ZyWALL, but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

29.8.5 Query Example

This example shows a search with these criteria:

- Severity: severe and high
- Attack Type: DDoS
- Platform: Windows 2000 and Windows XP computers
- Service: Any
- Actions: Any

Figure 327 Query Example Search Criteria



Attributes, hold "Ctrl" to make multiple selection on items in the list.

Severity: High, Severe

Attack Type: DDoS

Platform: WinXP/2000

Service: Any

Configured options

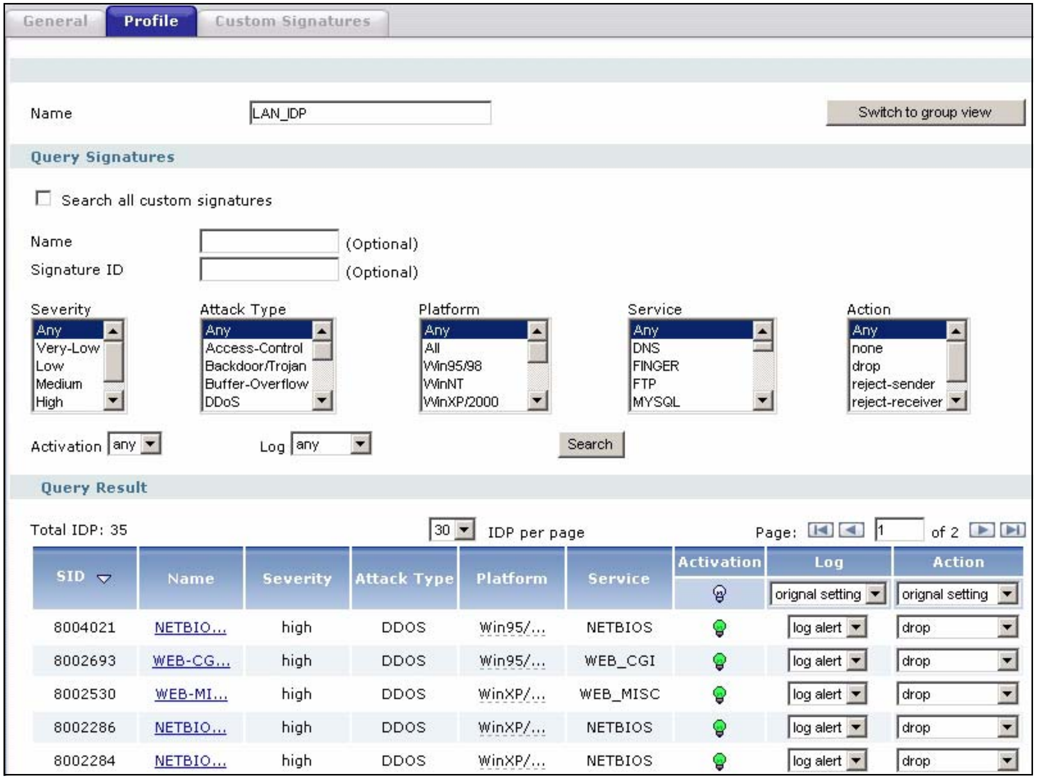
Activation: any

Log: any

Actions, hold "Ctrl" to make multiple selection on items in the list.

Any

Figure 328 Query Example Search Results



Name: LAN_IDP

☐ Search all custom signatures

Name (Optional)

Signature ID (Optional)

Severity: Any, Very-Low, Low, Medium, High

Attack Type: Any, Access-Control, Backdoor/Trojan, Buffer-Overflow, DDoS

Platform: Any, All, Win95/98, WinNT, WinXP/2000

Service: Any, DNS, FINGER, FTP, MYSQL

Action: Any, none, drop, reject-sender, reject-receiver

Activation: any

Log: any

Total IDP: 35

30 IDP per page

Page: 1 of 2

SID	Name	Severity	Attack Type	Platform	Service	Activation	Log	Action
							orignal setting	orignal setting
8004021	NETBIO...	high	DDOS	Win95/...	NETBIOS	●	log alert	drop
8002693	WEB-CG...	high	DDOS	Win95/...	WEB_CGI	●	log alert	drop
8002530	WEB-MI...	high	DDOS	WinXP/...	WEB_MISC	●	log alert	drop
8002286	NETBIO...	high	DDOS	WinXP/...	NETBIOS	●	log alert	drop
8002284	NETBIO...	high	DDOS	WinXP/...	NETBIOS	●	log alert	drop

29.9 Introducing IDP Custom Signatures

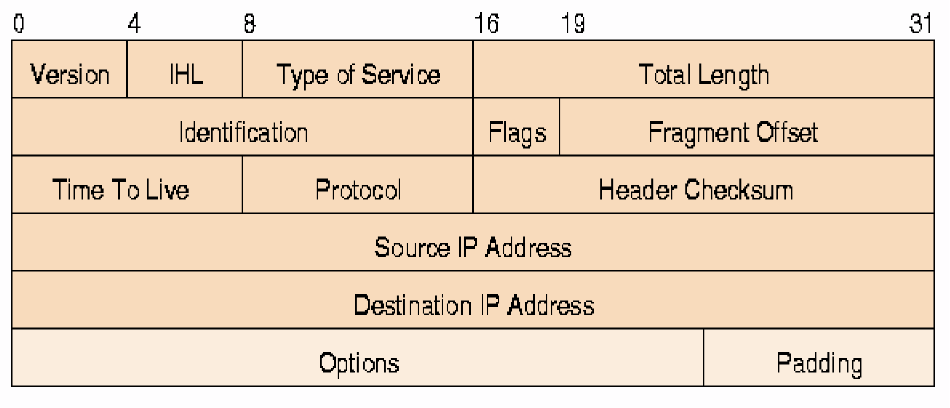
Create custom signatures for new attacks or attacks peculiar to your network. Custom signatures can also be saved to/from your computer so as to share with others.

You need some knowledge of packet headers and attack types to create your own custom signatures.

29.9.1 IP Packet Header

These are the fields in an Internet Protocol (IP) version 4 packet header.

Figure 329 IP v4 Packet Headers


0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time To Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
Options
Padding

The header fields are discussed below:

Table 135 IP v4 Packet Headers

HEADER	DESCRIPTION
Version	The value 4 indicates IP version 4.
IHL	IP Header Length is the number of 32 bit words forming the total length of the header (usually five).
Type of Service	The Type of Service, (also known as Differentiated Services Code Point (DSCP)) is usually set to 0, but may indicate particular quality of service needs from the network.
Total Length	This is the size of the datagram in bytes. It is the combined length of the header and the data.
Identification	This is a 16-bit number, which together with the source address, uniquely identifies this packet. It is used during reassembly of fragmented datagrams.
Flags	Flags are used to control whether routers are allowed to fragment a packet and to indicate the parts of a packet to the receiver.
Fragment Offset	This is a byte count from the start of the original sent packet.
Time To Live	This is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. It is used to prevent accidental routing loops.
Protocol	The protocol indicates the type of transport packet being carried, for example, 1 = ICMP; 2= IGMP; 6 = TCP; 17= UDP.
Header Checksum	This is used to detect processing errors introduced into the packet inside a router or bridge where the packet is not protected by a link layer cyclic redundancy check. Packets with an invalid checksum are discarded by all nodes in an IP network.
Source IP Address	This is the IP address of the original sender of the packet.
Destination IP Address	This is the IP address of the final destination of the packet.

Table 135 IP v4 Packet Headers (continued)

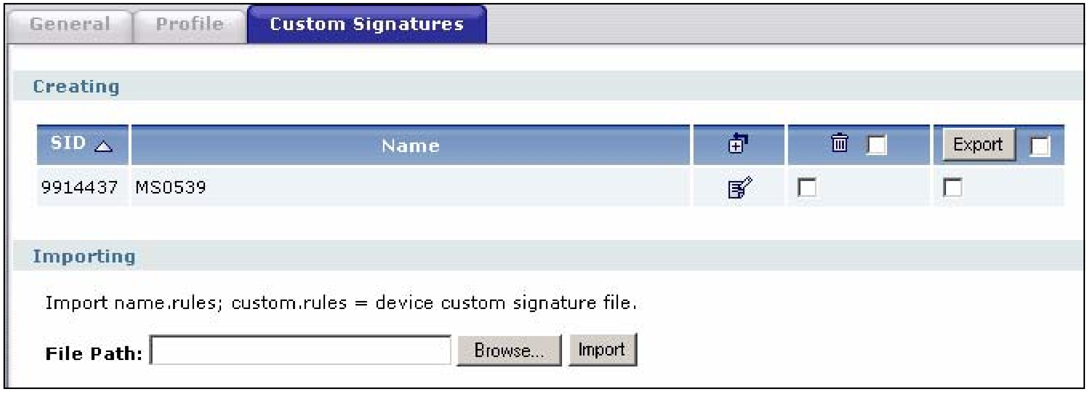
HEADER	DESCRIPTION
Options	IP options is a variable-length list of IP options for a datagram that define IP **Security Option**, **IP Stream Identifier**, (security and handling restrictions for the military), **Record Route** (have each router record its IP address), **Loose Source Routing** (specifies a list of IP addresses that must be traversed by the datagram), **Strict Source Routing** (specifies a list of IP addresses that must ONLY be traversed by the datagram), **Timestamp** (have each router record its IP address and time), **End of IP List** and **No IP Options**.
Padding	Padding is used as a filler to ensure that the IP packet is a multiple of 32 bits.

29.10 Configuring Custom Signatures

Select **Anti-X** > **IDP** > **Custom Signature**s. The first screen shows a summary of all custom signatures created. Click the **SID** or **Name** heading to sort. Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature. You can delete signatures here or save them to your computer.

The ZyWALL checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the ZyWALL applies the more restrictive action (**reject-both**, **reject-receiver or reject-sender**, **drop**, **none** in this order). If a packet matches a rule for **reject-receiver** and it also matches a rule for **reject-sender**, then the ZyWALL will **reject-both**.

Figure 330 Anti-X > IDP > Custom Signatures



SID △	Name		☐	Export ☐
9914437	MS0539		☐	☐

Import name.rules; custom.rules = device custom signature file.

File Path:

The following table describes the fields in this screen.

Table 136 Anti-X > IDP > Custom Signatures

LABEL	DESCRIPTION
Creating	Use this part of the screen to create, edit, delete or export (save to your computer) custom signatures.
SID	SID is the signature ID that uniquely identifies a signature. Click the SID header to sort signatures in ascending or descending order. It is automatically created when you click the **Add** icon to create a new signature. You can edit the ID, but it cannot already exist and it must be in the 9000000 to 9999999 range.
Name	This is the name of your custom signature. Duplicate names can exist, but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent.
Add/Edit	Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature.
Delete	Use this column to delete signatures. Select (or clear) the check box in the header column to select (or clear) all check boxes in that column. You can also select (or clear) individual signatures within the column. When you are certain that you have only selected signatures that you want to remove, click the **Delete** icon. Click **OK** in the confirm delete signature dialog box to delete the selected signature(s).
Export	Use this column to save signatures to your computer. Select (or clear) the check box in the header column to select (or clear) all check boxes in that column. You can also select (or clear) individual signatures within the column. When you are certain that you have only selected signatures that you want to save, click **Export**. Click **Save** in the file download dialog box and then select a location and name for the file. Custom signatures must end with the 'rules' file name extension, for example, MySig.rules.
Importing	Use this part of the screen to import custom signatures (previously saved to your computer) to the ZyWALL. Note: The name of the complete custom signature file on the ZyWALL is 'custom.rules'. If you import a file named 'custom.rules', then all custom signatures on the ZyWALL are overwritten with the new file. If this is not your intention, make sure that the files you import are not named 'custom.rules'.
File Path	Type the file path and name of the custom signature file you want to import in the text box (or click **Browse** to find it on your computer) and then click **Import** to transfer the file to the ZyWALL. New signatures then display in the ZyWALL **IDP > Custom Signatures** screen.

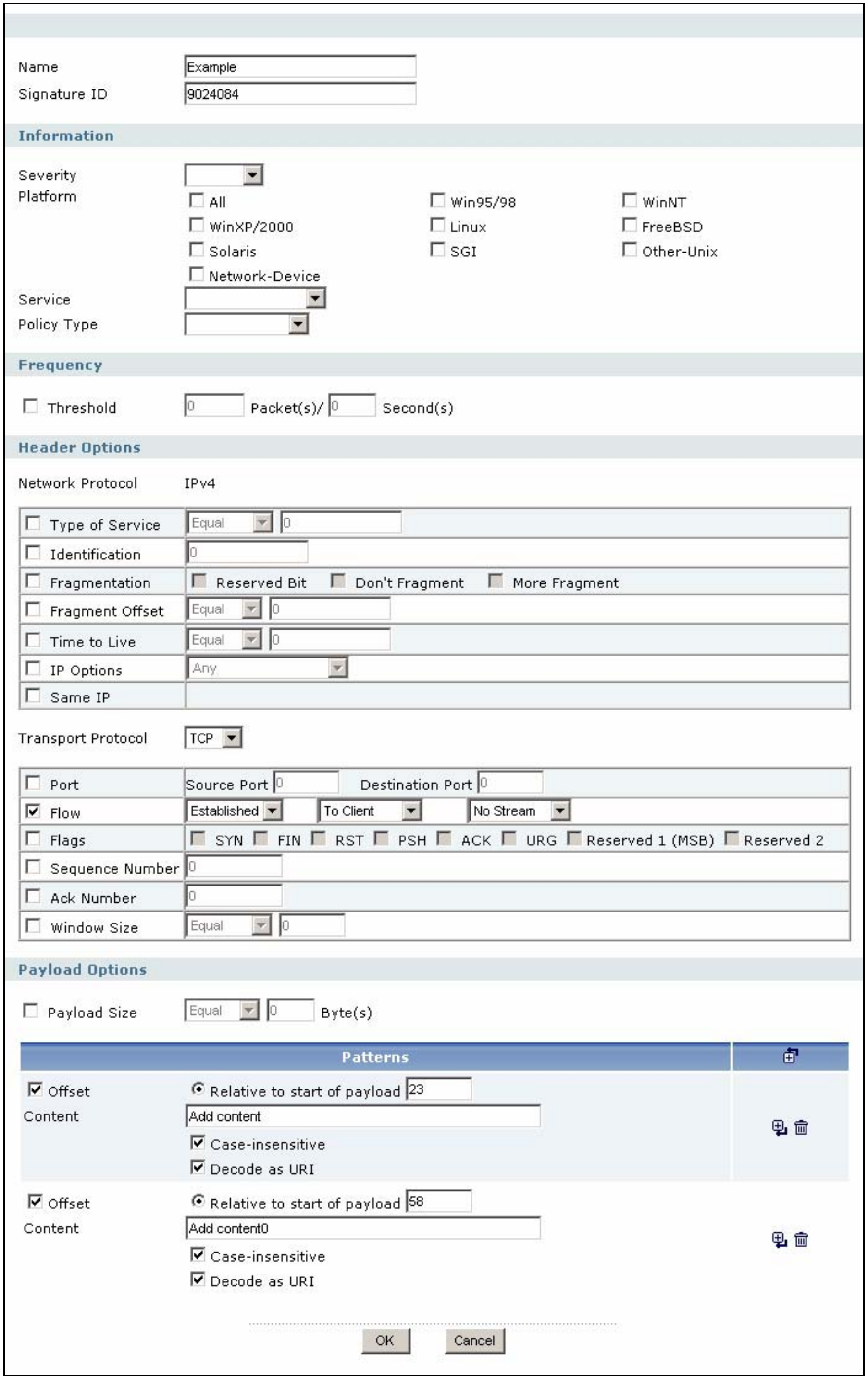
29.10.1 Creating or Editing a Custom Signature

Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature in the screen as shown in Figure 330 on page 434.

A packet must match all items you configure in this screen before it matches the signature. The more specific your signature (including packet contents), then the fewer false positives the signature will trigger.

Try to write signatures that target a vulnerability, for example a certain type of traffic on certain operating systems, instead of a specific exploit.

Figure 331 Anti-X > IDP > Custom Signatures > Add/Edit



Name: Example
Signature ID: 9024084

Information

Severity:
Platform: ☐ All ☐ Win95/98 ☐ WinNT ☐ WinXP/2000 ☐ Linux ☐ FreeBSD ☐ Solaris ☐ SGI ☐ Other-Unix ☐ Network-Device
Service:
Policy Type:

Frequency

☐ Threshold 0 Packet(s)/ 0 Second(s)

Header Options

Network Protocol: IPv4

☐ Type of Service: Equal 0
☐ Identification: 0
☐ Fragmentation: ☐ Reserved Bit ☐ Don't Fragment ☐ More Fragment
☐ Fragment Offset: Equal 0
☐ Time to Live: Equal 0
☐ IP Options: Any
☐ Same IP

Transport Protocol: TCP

☐ Port: Source Port 0 Destination Port 0
☑ Flow: Established, To Client, No Stream
☐ Flags: ☐ SYN ☐ FIN ☐ RST ☐ PSH ☐ ACK ☐ URG ☐ Reserved 1 (MSB) ☐ Reserved 2
☐ Sequence Number: 0
☐ Ack Number: 0
☐ Window Size: Equal 0

Payload Options

☐ Payload Size: Equal 0 Byte(s)

Patterns

☑ Offset: ● Relative to start of payload 23
Content: Add content
☑ Case-insensitive
☑ Decode as URI

☑ Offset: ● Relative to start of payload 58
Content: Add content0
☑ Case-insensitive
☑ Decode as URI

The following table describes the fields in this screen.

Table 137 Anti-X > IDP > Custom Signatures > Add/Edit

LABEL	DESCRIPTION
Name	Type the name of your custom signature. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. Duplicate names can exist but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent. Refer to (but do not copy) the packet inspection signature names for hints on creating a naming convention.
Signature ID	A signature ID is automatically created when you click the **Add** icon to create a new signature. You can edit the ID to create a new one (in the 9000000 to 9999999 range), but you cannot use one that already exists. You may want to do that if you want to order custom signatures by SID.
Information	Use the following fields to set general information about the signature as denoted below.
Severity	The severity level denotes how serious the intrusion is. Categorize the seriousness of the intrusion here. See Table 131 on page 426 as a reference.
Platform	Some intrusions target specific operating systems only. Select the operating systems that the intrusion targets, that is, the operating systems you want to protect from this intrusion. SGI refers to Silicon Graphics Incorporated, who manufactures multi-user Unix workstations that run the IRIX operating system (SGI's version of UNIX). A router is an example of a network device.
Service	Select the IDP service group that the intrusion exploits or targets. See Table 133 on page 428 for a list of IDP service groups. The custom signature then appears in that group in the **IDP > Profile > Group View** screen.
Policy Type	Categorize the type of intrusion here. See Table 132 on page 427 as a reference.
Frequency	Recurring packets of the same type may indicate an attack. Use the following field to indicate how many packets per how many seconds constitute an intrusion
Threshold	Select **Threshold** and then type how many packets (that meet the criteria in this signature) per how many seconds constitute an intrusion.
Header Options	
Network Protocol	Configure signatures for IP version 4.
Type Of Service	Type of service in an IP header is used to specify levels of speed and/or reliability. Some intrusions use an invalid **Type Of Service** number. Select the check box, then select **Equal** or **Not-Equal** and then type in a number.
Identification	The identification field in a datagram uniquely identifies the datagram. If a datagram is fragmented, it contains a value that identifies the datagram to which the fragment belongs. Some intrusions use an invalid **Identification** number. Select the check box and then type in the invalid number that the intrusion uses.
Fragmentation	A fragmentation flag identifies whether the IP datagram should be fragmented, not fragmented or is a reserved bit. Some intrusions can be identified by this flag. Select the check box and then select the flag that the intrusion uses.
Fragmentation Offset	When an IP datagram is fragmented, it is reassembled at the final destination. The fragmentation offset identifies where the fragment belongs in a set of fragments. Some intrusions use an invalid **Fragmentation Offset** number. Select the check box, select **Equal**, **Smaller** or **Greater** and then type in a number
Time to Live	Time to Live is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. Usually it’s used to set an upper limit on the number of routers a datagram can pass through. Some intrusions can be identified by the number in this field. Select the check box, select **Equal**, **Smaller** or **Greater** and then type in a number.

Table 137 Anti-X > IDP > Custom Signatures > Add/Edit (continued)

LABEL	DESCRIPTION
IP Options	IP options is a variable-length list of IP options for a datagram that define IP **Security Option, IP Stream Identifier**, (security and handling restrictions for the military), **Record Route** (have each router record its IP address), **Loose Source Routing** (specifies a list of IP addresses that must be traversed by the datagram), **Strict Source Routing** (specifies a list of IP addresses that must ONLY be traversed by the datagram), **Timestamp** (have each router record its IP address and time), **End of IP List** and **No IP Options**. **IP Options** can help identify some intrusions. Select the check box, then select an item from the list box that the intrusion uses
Same IP	Select the check box for the signature to check for packets that have the same source and destination IP addresses.
Transport Protocol	The following fields vary depending on whether you choose **TCP**, **UDP** or **ICMP**.
Transport Protocol: TCP	
Port	Select the check box and then enter the source and destination TCP port numbers that will trigger this signature.
Flow	If selected, the signature only applies to certain directions of the traffic flow and only to clients or servers. Select **Flow** and then select the identifying options. **Established**: The signature only checks for established TCP connections **Stateless**: The signature is triggered regardless of the state of the stream processor (this is useful for packets that are designed to cause devices to crash) **To Client**: The signature only checks for server responses from A to B. **To Server**: The signature only checks for client requests from B to A. **From Client**:.The signature only checks for client requests from B to A. **From Servers**: The signature only checks for server responses from A to B. **No Stream**: The signature does not check rebuilt stream packets. **Only Stream**: The signature only checks rebuilt stream packets.
Flags	Select what TCP flag bits the signature should check.
Sequence Number	Use this field to check for a specific TCP sequence number.
Ack Number	Use this field to check for a specific TCP acknowledgement number.
Window Size	Use this field to check for a specific TCP window size.
Transport Protocol: UDP	
Port	Select the check box and then enter the source and destination UDP port numbers that will trigger this signature.
Transport Protocol: ICMP	
Type	Use this field to check for a specific ICMP type value.
Code	Use this field to check for a specific ICMP code value.
ID	Use this field to check for a specific ICMP ID value. This is useful for covert channel programs that use static ICMP fields when they communicate.
Sequence Number	Use this field to check for a specific ICMP sequence number. This is useful for covert channel programs that use static ICMP fields when they communicate.
Payload Options	The longer a payload option is, the more exact the match, the faster the signature processing. Therefore, if possible, it is recommended to have at least one payload option in your signature.

Table 137 Anti-X > IDP > Custom Signatures > Add/Edit (continued)

LABEL	DESCRIPTION
Payload Size	This field may be used to check for abnormally sized packets or for detecting buffer overflows. Select the check box, then select **Equal**, **Smaller** or **Greater** and then type the payload size. Stream rebuilt packets are not checked regardless of the size of the payload.
Offset	This field specifies where to start searching for a pattern within a packet. For example, an offset of 5 would start looking for the specified pattern after the first five bytes of the payload.
Content	Type the content that the signature should search for in the packet payload. Hexadecimal code entered between pipes is converted to ASCII. For example, you could represent the ampersand as either & or |26| (26 is the hexadecimal code for the ampersand).
Case-insensitive	Select this check box if content casing does NOT matter.
Decode as URI	A Uniform Resource Identifier (URI) is a string of characters for identifying an abstract or physical resource (RFC 2396). A resource can be anything that has identity, for example, an electronic document, an image, a service ("today's weather report for Taiwan"), a collection of other resources. An identifier is an object that can act as a reference to something that has identity. Example URIs are: ftp://ftp.is.co.za/rfc/rfc1808.txt; ftp scheme for File Transfer Protocol services http://www.math.uio.no/faq/compression-faq/part1.html; http scheme for Hypertext Transfer Protocol services mailto:mduerst@ifi.unizh.ch; mailto scheme for electronic mail addresses telnet://melvyl.ucop.edu/; telnet scheme for interactive services via the TELNET Protocol Select this check box for the signature to search for normalized URI fields. This means that if you are writing signatures that includes normalized content, such as %2 for directory traversals, these signatures will not be triggered because the content is normalized out of the URI buffer. For example, the URI: /scripts/..%c0%af../winnt/system32/cmd.exe?/c+ver will get normalized into: /winnt/system32/cmd.exe?/c+ver
OK	Click this button to save your changes to the ZyWALL and return to the summary screen.
Cancel	Click this button to return to the summary screen without saving any changes.

29.10.2 Custom Signature Example

Before creating a custom signature, you must first clearly understand the vulnerability.

29.10.2.1 Understand the Vulnerability

Check the ZyWALL logs when the attack occurs. Use web sites such as Google and security focus to get as much information about the attack as you can. The more specific your signature, the less chance it will cause false positives.

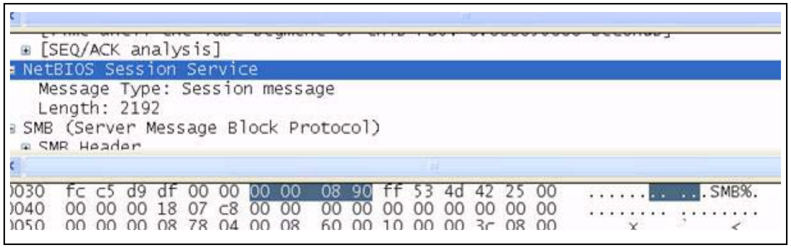
As an example, say you want to create a signature for the 'Microsoft Windows Plug-and-Play Service Remote Overflow (MS-05-39)' attack. Search the Security Focus web site and you will find it uses the NetBIOS service in established TCP connections to a server using port 445.

29.10.2.2 Analyze Packets

Then use a packet sniffer such as TCPdump or Ethereal to investigate some more.

From the NetBIOS header you see that the first byte ‘00’ defines the message type. The next three bytes represent the length of data, so you can ignore it. Therefore enter **|00|** as the first pattern.

Figure 332 Custom Signature Example Pattern 1

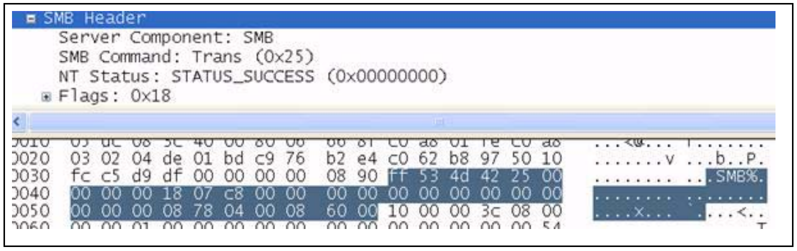


```
  [SEQ/ACK analysis]
NetBIOS Session Service
   Message Type: Session message
   Length: 2192
SMB (Server Message Block Protocol)
  SMB Header

0030  fc c5 d9 df 00 00 00 00  08 90 ff 53 4d 42 25 00   ........ ..SMB%.
0040  00 00 00 18 07 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 08 78 04 00 08  60 00 10 00 00 3c 08 00   ....x...  ....<..
```

Next, check the content of the SMB header. Add **|FF|SMB%** and ‘TransactionNmPipe’ to the signature as the next patterns.

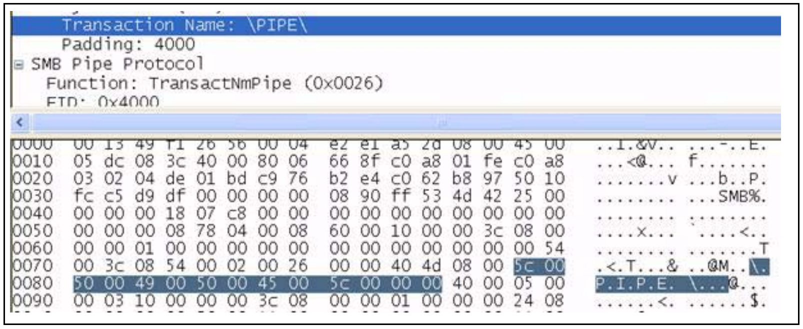
Figure 333 Custom Signature Example Pattern 2



```
SMB Header
    Server Component: SMB
    SMB Command: Trans (0x25)
    NT Status: STATUS_SUCCESS (0x00000000)
  Flags: 0x18

0010  05 dc 08 3c 40 00 80 06  66 8f c0 a8 01 fe c0 a8   ...<@... f.......
0020  03 02 04 de 01 bd c9 76  b2 e4 c0 62 b8 97 50 10   .......v ...b..P.
0030  fc c5 d9 df 00 00 00 00  08 90 ff 53 4d 42 25 00   ........ ...SMB%.
0040  00 00 00 18 07 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 08 78 04 00 08  60 00 10 00 00 3c 08 00   ....x...  ....<..
0060  00 00 01 00 00 00 00 00  00 00 00 00 00 00 00 54   ........ .......T
```

Figure 334 Custom Signature Example Patterns 3 and 4



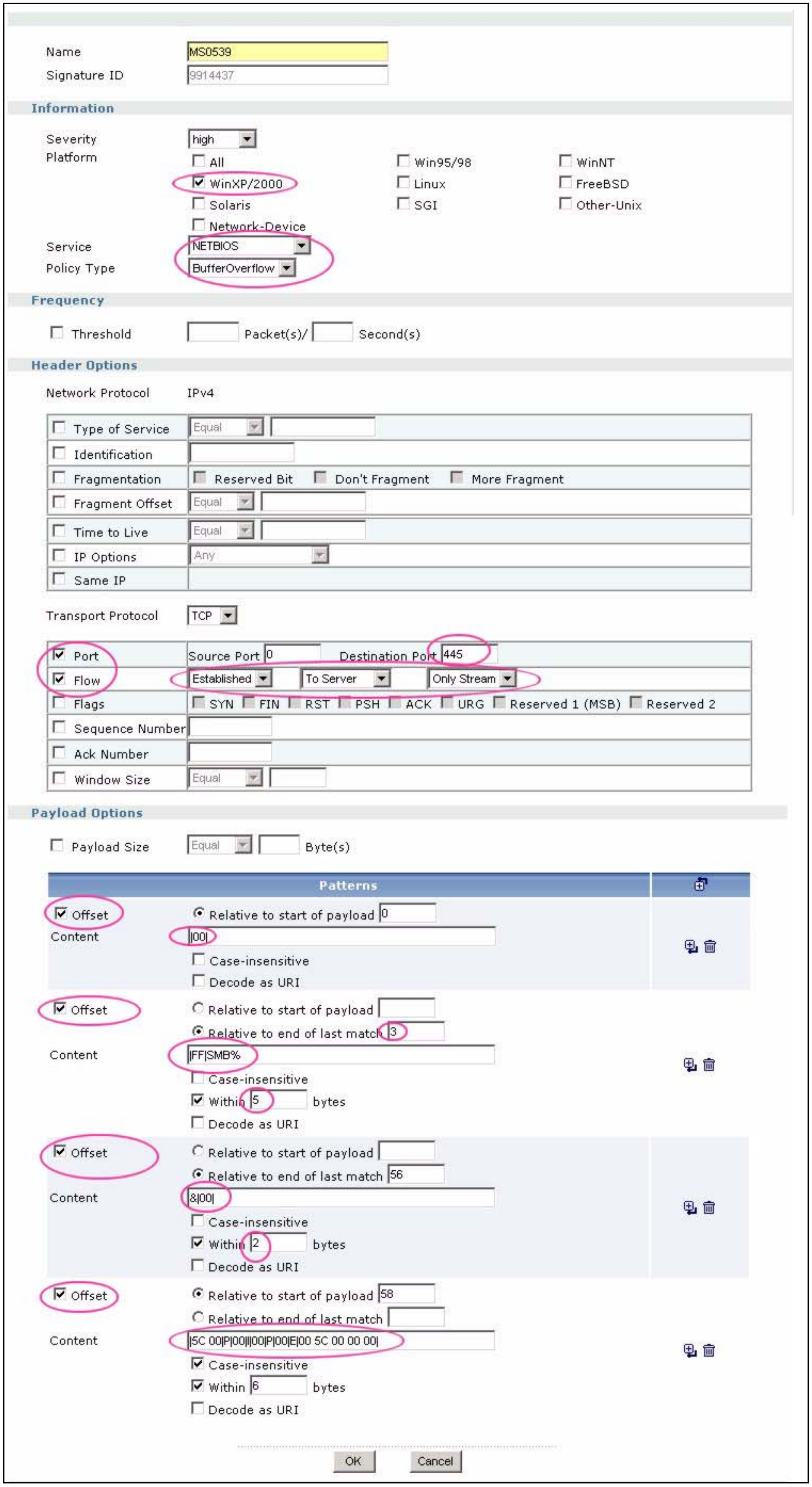
```
    Transaction Name: \PIPE\
    Padding: 4000
SMB Pipe Protocol
   Function: TransactNmPipe (0x0026)
   FID: 0x4000

0000  00 13 49 f1 26 56 00 04  e2 e1 a5 2d 08 00 45 00   ..I.&V.. ...-..E.
0010  05 dc 08 3c 40 00 80 06  66 8f c0 a8 01 fe c0 a8   ...<@... f.......
0020  03 02 04 de 01 bd c9 76  b2 e4 c0 62 b8 97 50 10   .......v ...b..P.
0030  fc c5 d9 df 00 00 00 00  08 90 ff 53 4d 42 25 00   ........ ...SMB%.
0040  00 00 00 18 07 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 08 78 04 00 08  60 00 10 00 00 3c 08 00   ....x...  ....<..
0060  00 00 01 00 00 00 00 00  00 00 00 00 00 00 00 54   ........ .......T
0070  00 3c 08 54 00 02 00 26  00 00 40 4d 08 00 5c 00   .<.T...& ..@M..\.
0080  50 00 49 00 50 00 45 00  5c 00 00 00 40 00 05 00   P.I.P.E. \...@...
0090  00 03 10 00 00 00 3c 08  00 00 01 00 00 00 24 08   ......<. ......$.
```

Our final custom signature should look like as shown in the following figure.

If the attack occurs, check the logs for a log of your custom signature. This indicates the signature works correctly.

Figure 335 Example Custom Signature



Name: MS0539
Signature ID: 9914437

Information

Severity: high
Platform:
☐ All ☐ Win95/98 ☐ WinNT
☑ WinXP/2000 ☐ Linux ☐ FreeBSD
☐ Solaris ☐ SGI ☐ Other-Unix
☐ Network-Device
Service: NETBIOS
Policy Type: BufferOverflow

Frequency

☐ Threshold Packet(s)/ Second(s)

Header Options

Network Protocol: IPv4

☐ Type of Service: Equal
☐ Identification
☐ Fragmentation: ☐ Reserved Bit ☐ Don't Fragment ☐ More Fragment
☐ Fragment Offset: Equal
☐ Time to Live: Equal
☐ IP Options: Any
☐ Same IP

Transport Protocol: TCP

☑ Port: Source Port 0 Destination Port 445
☑ Flow: Established, To Server, Only Stream
☐ Flags: ☐ SYN ☐ FIN ☐ RST ☐ PSH ☐ ACK ☐ URG ☐ Reserved 1 (MSB) ☐ Reserved 2
☐ Sequence Number
☐ Ack Number
☐ Window Size: Equal

Payload Options

☐ Payload Size: Equal Byte(s)

Patterns

☑ Offset: ● Relative to start of payload 0
Content: |00|
☐ Case-insensitive
☐ Decode as URI

☑ Offset: ○ Relative to start of payload; ● Relative to end of last match 3
Content: |FF|SMB%
☐ Case-insensitive
☑ Within 5 bytes
☐ Decode as URI

☑ Offset: ○ Relative to start of payload; ● Relative to end of last match 56
Content: &|00|
☐ Case-insensitive
☑ Within 2 bytes
☐ Decode as URI

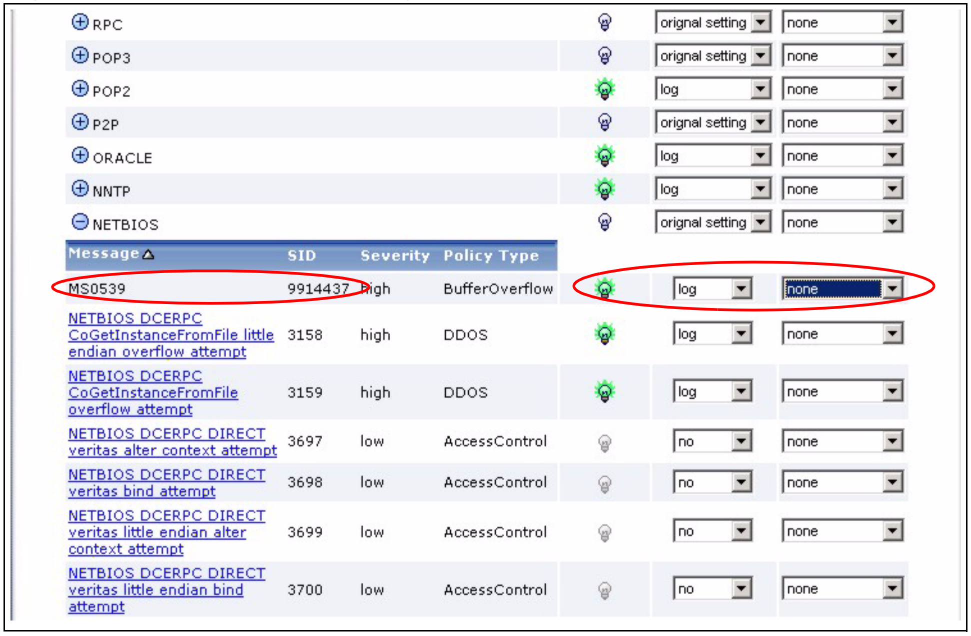
☑ Offset: ● Relative to start of payload 58; ○ Relative to end of last match
Content: |5C 00|P|00|I|00|P|00|E|00 5C 00 00 00|
☑ Case-insensitive
☑ Within 6 bytes
☐ Decode as URI

29.10.3 Applying Custom Signatures

After you create your custom signature, it becomes available in the IDP service group category in the **IDP** > **Profile** > **Packet Inspection** screen. Custom signatures have an SID from 9000000 to 9999999.

You can activate the signature, configure what action to take when a packet matches it and if it should generate a log or alert in a profile. Then bind the profile to a zone.

Figure 336 Example: Custom Signature in IDP Profile



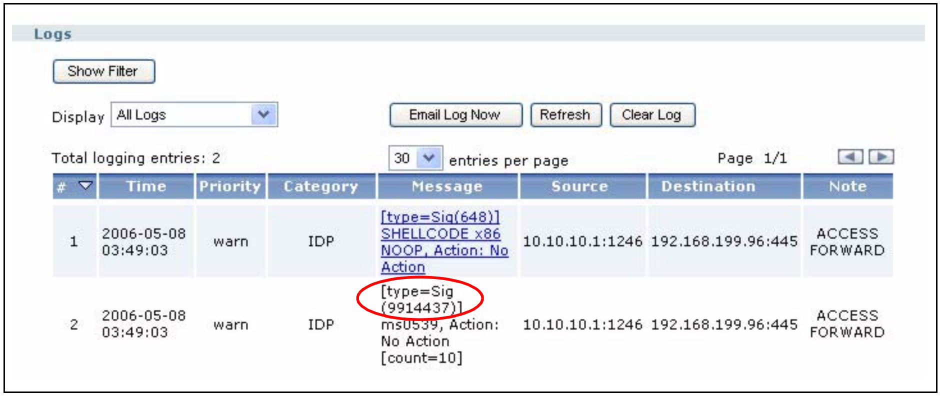
Message	SID	Severity	Policy Type			
⊕ RPC				○	orignal setting	none
⊕ POP3				○	orignal setting	none
⊕ POP2				●	log	none
⊕ P2P				○	orignal setting	none
⊕ ORACLE				●	log	none
⊕ NNTP				●	log	none
⊖ NETBIOS				○	orignal setting	none
MS0539	9914437	high	BufferOverflow	●	log	none
NETBIOS DCERPC CoGetInstanceFromFile little endian overflow attempt	3158	high	DDOS	●	log	none
NETBIOS DCERPC CoGetInstanceFromFile overflow attempt	3159	high	DDOS	●	log	none
NETBIOS DCERPC DIRECT veritas alter context attempt	3697	low	AccessControl	○	no	none
NETBIOS DCERPC DIRECT veritas bind attempt	3698	low	AccessControl	○	no	none
NETBIOS DCERPC DIRECT veritas little endian alter context attempt	3699	low	AccessControl	○	no	none
NETBIOS DCERPC DIRECT veritas little endian bind attempt	3700	low	AccessControl	○	no	none

29.10.4 Verifying Custom Signatures

You should configure the signature to create a log when an ‘attack packet’ matches the signature. (You may also want to configure an alert if the attack is more serious and needs more immediate attention.) After you apply the signature to a zone, you can see if it works by checking the logs (**Maintenance** > **Logs** > **View Log**).

All IDP signatures come under the **IDP** category. The **Priority** column shows **warn** for signatures that are configured to generate a log only. It shows **critical** for signatures that are configured to generate a log and alert. **count** is the number of attacks that occurred at that time. The **Note** column displays **ACCESS FORWARD** when no action is configured for the signature. It displays **ACCESS DENIED** if you configure the signature action to drop the packet. The destination port is the service port (NetBIOS in this case) that the attack tries to exploit.

Figure 337 Custom Signature Log



Total logging entries: 2

30 entries per page Page 1/1

#	Time	Priority	Category	Message	Source	Destination	Note
1	2006-05-08 03:49:03	warn	IDP	[type=Sig(648)] SHELLCODE x86 NOOP, Action: No Action	10.10.10.1:1246	192.168.199.96:445	ACCESS FORWARD
2	2006-05-08 03:49:03	warn	IDP	[type=Sig (9914437)] ms0539, Action: No Action [count=10]	10.10.10.1:1246	192.168.199.96:445	ACCESS FORWARD

29.10.5 Snort Signatures

You may want to refer to open source Snort signatures when creating custom ZyWALL ones. Most Snort rules are written in a single line. Snort rules are divided into two logical sections, the rule header and the rule options as shown in the following example:

```
alert tcp any any -> 192.168.1.0/24 111 (content:”|00 01 a5|”;
msg:”mountd access”;)
```

The text up to the first parenthesis is the rule header and the section enclosed in parenthesis contains the rule options. The words before the colons in the rule options section are the option keywords.

The rule header contains the rule's:

- Action
- Protocol
- Source and destination IP addresses and netmasks
- Source and destination ports information.

The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

These are some equivalent Snort terms in the ZyWALL.

Table 138 ZyWALL - Snort Equivalent Terms

ZYWALL TERM	SNORT EQUIVALENT TERM
Type Of Service	tos
Identification	id
Fragmentation	fragbits
Fragmentation Offset	fragoffset
Time to Live	ttl
IP Options	ipopts
Same IP	sameip
Transport Protocol	
Transport Protocol: TCP	
Port	(In Snort rule header)

Table 138 ZyWALL - Snort Equivalent Terms (continued)

ZYWALL TERM	SNORT EQUIVALENT TERM
Flow	flow
Flags	flags
Sequence Number	seq
Ack Number	ack
Window Size	window
Transport Protocol: UDP	(In Snort rule header)
Port	(In Snort rule header)
Transport Protocol: ICMP	
Type	itype
Code	icode
ID	icmp_id
Sequence Number	icmp_seq
Payload Options	(Snort rule options)
Payload Size	dsize
Offset (relative to start of payload)	offset
Relative to end of last match	distance
Content	content
Case-insensitive	nocase
Decode as URI	uricontent

Not all Snort functionality is supported in the ZyWALL.

30

ADP

This chapter introduces ADP (Anomaly Detection and Prevention), anomaly profiles and binding an ADP profile to a traffic direction. See Section 5.4.16 on page 120 for related information on these screens.

30.1 Introduction to ADP

An ADP system can detect malicious or suspicious packets and respond instantaneously. It can detect:

- Anomalies based on violations of protocol standards (RFCs – Requests for Comments)
- Abnormal flows such as port scans.

30.1.1 Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install a host ADP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host ADPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

30.1.2 Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda MyDoom etc.

30.1.3 ADP on the ZyWALL

ADP on the ZyWALL protects against network-based intrusions. See Section 30.8 on page 450 and Section 30.9 on page 456 for more on the kinds of attacks that the ZyWALL can protect against. You can also create your own custom ADP rules.

30.2 Traffic Directions and Profiles

A zone is a combination of ZyWALL interfaces and VPN connections for security. See the zone chapter for details on zones and the interfaces chapter for details on interfaces. Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to.

An anomaly profile is a set of ADP rules with configured activation, log and action settings. The ZyWALL comes with default profiles that you can bind to traffic directions. For example, by default, the default LAN_ADP profile is bound to any traffic going to the LAN zone. You could use this to protect your LAN computers.

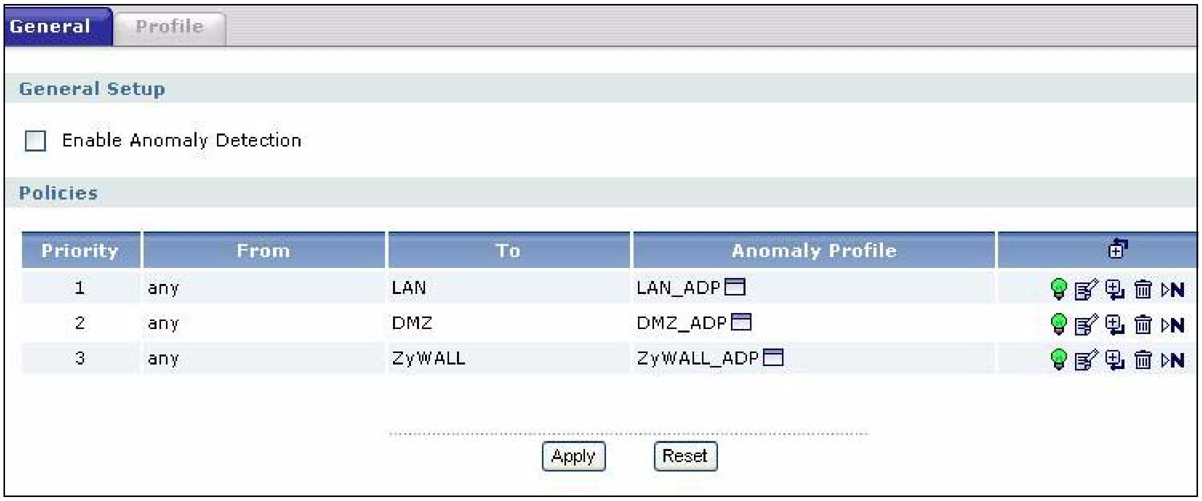
You can also create your own ADP profiles from base profiles. See Table 141 on page 449 for details on base profiles.

You can only bind one profile to one traffic direction.

30.3 Configuring ADP General

Click **Anti-X** > **ADP** > **General**. Use this screen to turn anomaly detection on or off and bind anomaly profiles to traffic directions.

Figure 338 Anti-X > ADP > General



General Setup

☐ Enable Anomaly Detection

Policies

Priority	From	To	Anomaly Profile
1	any	LAN	LAN_ADP
2	any	DMZ	DMZ_ADP
3	any	ZyWALL	ZyWALL_ADP

The following table describes the screens in this screen.

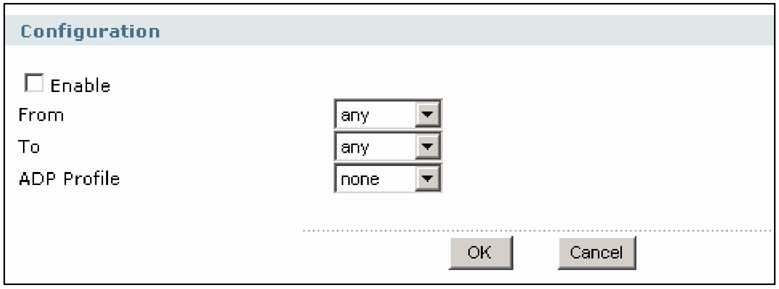
Table 139 Anti-X > ADP > General

LABEL	DESCRIPTION
General Setup	
Enable Anomaly Detection	Select this check box to enable traffic anomaly and protocol anomaly detection.
Bindings	Use this list to specify which anomaly profile the ZyWALL uses for traffic flowing in a specific direction.
Priority	This is this binding's rank in the list of anomaly profile to traffic direction bindings. The list is applied in order of priority.
From, To	This is the direction of travel of packets to which an anomaly profile is bound. Note: Depending on your network topology and traffic load, binding every packet direction to an anomaly profile may affect the ZyWALL's performance. **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet via the ZyWALL's LAN zone interfaces. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet. **From WAN To WAN** means packets that come in from the WAN zone and the ZyWALL routes back out through the WAN zone.
Anomaly Profile	An anomaly profile is a set of anomaly rules with configured activation, log and action settings. This field shows which anomaly profile is bound to which traffic direction.
(Icons)	Click the **Add** icon in the heading row to add a new first entry. The **Active** icon displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Add** icon in an entry to add an entry below the current entry. Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action. In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one. The ordering of your entries is important as they are applied in order of their numbering.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to start configuring this screen again.

30.4 Configuring Anomaly Profile Bindings

Click **Anti-X > ADP > General** and then an **Add** or **Edit** icon to display the following screen. Use this screen to bind an anomaly profile to a traffic direction.

Figure 339 Anti-X > ADP > General > Add



Configuration

☐ Enable

From: any

To: any

ADP Profile: none

The following table describes the screens in this screen.

Table 140 Anti-X > ADP > General > Add

LABEL	DESCRIPTION
Enable	Select this check box to turn on this anomaly profile to traffic direction binding.
From	Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to. Use the **From** field to specify the zone from which the traffic is coming. Select **ZyWALL** to specify traffic coming from the ZyWALL itself.
To	Use the **To** field to specify the zone to which the traffic is going. Select **ZyWALL** to specify traffic destined for the ZyWALL itself.
ADP Profile	An ADP profile is a set of ADP rules with configured activation, log and action settings. Select an ADP profile to bind to the entry's traffic direction. Configure the ADP profiles in the ADP profile screens.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

30.5 Introducing ADP Profiles

An ADP profile is a set of traffic anomaly rules and protocol anomaly rules.

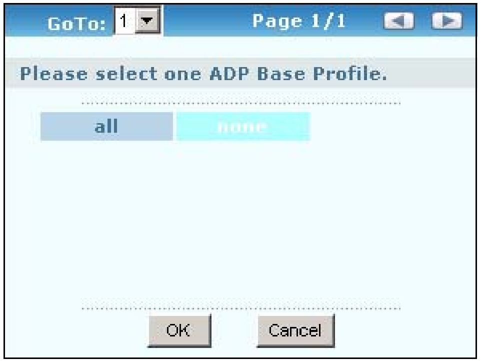
- Traffic anomaly rules look for abnormal behavior or events such as port scanning, sweeping or network flooding. It operates at OSI layer-2 and layer-3. Traffic anomaly rules may be updated when you upload new firmware.
- Protocol anomaly rules check for protocol compliance against the relevant RFC (Request For Comments). Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder. Protocol anomaly rules may be updated when you upload new firmware.

Anomaly detection is in general effective against abnormal behavior while packet inspection signatures are created for known attacks (see Chapter 29 on page 417 for information on packet inspection).

30.5.1 Base Profiles

The ZyWALL comes with several base profiles. You use base profiles to create new profiles.

Figure 340 Base Profiles



These are the default base profiles at the time of writing.

Table 141 Base Profiles

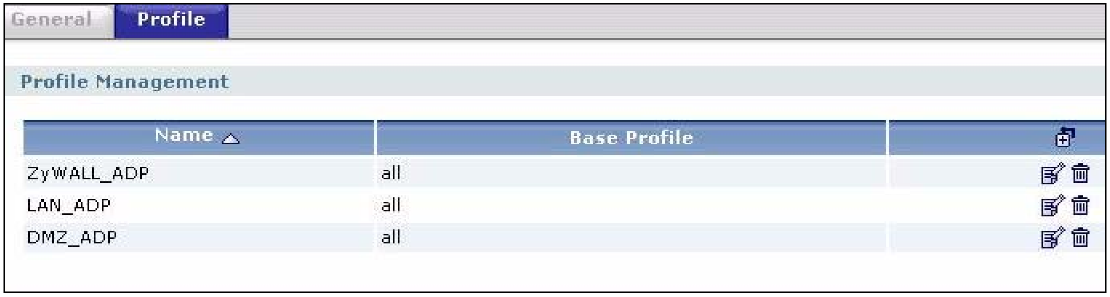
BASE PROFILE	DESCRIPTION
all	All traffic anomaly and protocol anomaly rules are enabled. Rules with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Rules with a very low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them.
none	All traffic anomaly and protocol anomaly rules are disabled. No logs are generated nor actions are taken.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

30.6 Profile Summary Screen

Select **Anti-X** > **ADP** > **Profile**. Use this screen to:

- Add a new profile
- Edit an existing profile
- Delete an existing profile

Figure 341 Anti-X > ADP > Profile



Name	Base Profile
ZyWALL_ADP	all
LAN_ADP	all
DMZ_ADP	all

The following table describes the fields in this screen.

Table 142 Anti-X > ADP > Profile

LABEL	DESCRIPTION
Name	This is the name of the profile you created.

Table 142 Anti-X > ADP > Profile (continued)

LABEL	DESCRIPTION
Base Profile	This is the base profile from which the profile was created.
(Icons)	Click the **Add** icon in the column header to create a new profile. A pop-up screen displays requiring you to choose a base profile from which to create the new profile. Click an **Edit** icon to edit an existing profile. Click a **Remove** icon to delete an existing profile.

30.7 Creating New Profiles

You may want to create a new profile if not all rules in a base profile are applicable to your network. In this case you should disable non-applicable rules so as to improve ZyWALL ADP processing efficiency.

You may also find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL. As each network is different, false positives and false negatives are common on initial ADP deployment.

You could create a new ‘monitor profile’ that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you’re satisfied that they have been reduced to an acceptable level, you could then create an ‘inline profile’ whereby you configure appropriate actions to be taken when a packet matches a rule.

30.7.1 Procedure To Create a New Profile

To create a new profile:

1. Click the **Add** icon in the **Anti-X** > **ADP** > **Profile** screen to display a pop-up screen allowing you to choose a base profile.
2. Select a base profile (see Table 141 on page 449) and then click **OK** to go to the profile details screen.
3. Type a new profile name
4. Enable or disable individual rules
5. Edit the default log options and actions.

30.8 Profiles: Traffic Anomaly

The traffic anomaly screen is the second screen in an ADP profile. Traffic anomaly detection looks for abnormal behavior such as scan or flooding attempts. In the **Anti-X** > **ADP** > **Profile** screen, click the **Edit** icon or click the **Add** icon and choose a base profile. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Traffic Anomaly** tab.

30.8.1 Port Scanning

An attacker scans device(s) to determine what types of network protocols or services a device supports. One of the most common port scanning tools in use today is Nmap.

Many connection attempts to different ports (services) may indicate a port scan. These are some port scan types:

- TCP Portscan
- UDP Portscan
- IP Portscan

An IP port scan searches not only for TCP, UDP and ICMP protocols in use by the remote computer, but also additional IP protocols such as EGP (Exterior Gateway Protocol) or IGP (Interior Gateway Protocol). Determining these additional protocols can help reveal if the destination device is a workstation, a printer, or a router.

30.8.1.1 Decoy Port Scans

Decoy port scans are scans where the attacker has spoofed the source address. These are some decoy scan types:

- TCP Decoy Portscan
- UDP Decoy Portscan
- IP Decoy Portscan

30.8.1.2 Distributed Port Scans

Distributed port scans are many-to-one port scans. Distributed port scans occur when multiple hosts query one host for open services. This may be used to evade intrusion detection. These are distributed port scan types:

- TCP Distributed Portscan
- UDP Distributed Portscan
- IP Distributed Portscan

30.8.1.3 Port Sweeps

Many different connection attempts to the same port (service) may indicate a port sweep, that is, they are one-to-many port scans. One host scans a single port on multiple hosts. This may occur when a new exploit comes out and the attacker is looking for a specific service. These are some port sweep types:

- TCP Portsweep
- UDP Portsweep
- IP Portsweep
- ICMP Portsweep

30.8.1.4 Filtered Port Scans

A filtered port scan may indicate that there were no network errors (ICMP unreachables or TCP RSTs) or responses on closed ports have been suppressed. Active network devices, such as NAT routers, may trigger these alerts if they send out many connection attempts within a very small amount of time. These are some filtered port scan examples.

- TCP Filtered Portscan
- UDP Filtered Portscan
- IP Filtered Portscan
- TCP Filtered Decoy Portscan
- UDP Filtered Decoy Portscan
- IP Filtered Decoy Portscan
- TCP Filtered Portsweep
- UDP Filtered Portsweep
- IP Filtered Portsweep
- ICMP Filtered Portsweep
- TCP Filtered Distributed Portscan
- UDP Filtered Distributed Portscan
- IP Filtered Distributed Portscan

30.8.2 Flood Detection

Flood attacks saturate a network with useless data, use up all available bandwidth, and therefore make communications in the network impossible.

30.8.2.1 ICMP Flood Attack

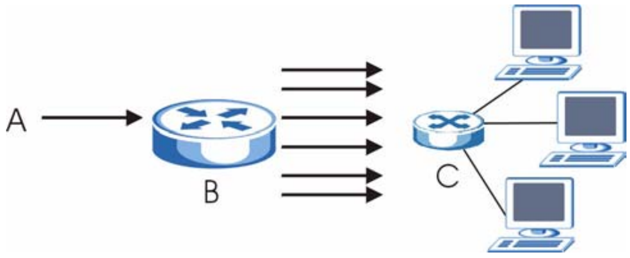
An ICMP flood is broadcasting many pings or UDP packets so that so much data is sent to the system, that it slows it down or locks it up.

30.8.2.2 Smurf

A smurf attacker (A) floods a router (B) with Internet Control Message Protocol (ICMP) echo request packets (pings) with the destination IP address of each packet as the broadcast address of the network. The router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic.

If an attacker (A) spoofs the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only saturate the receiving network (B), but the network of the spoofed source IP address (C).

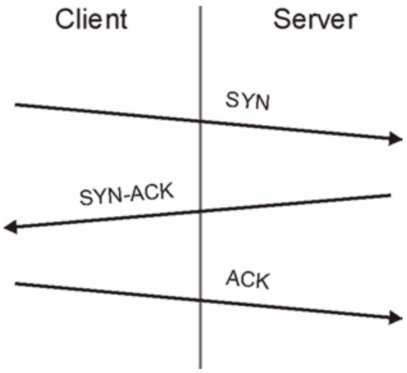
Figure 342 Smurf Attack



30.8.2.3 TCP SYN Flood Attack

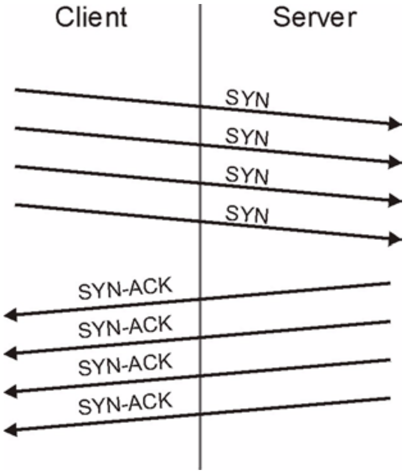
Usually a client starts a session by sending a SYN (synchronize) packet to a server. The receiver returns an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 343 TCP Three-Way Handshake



A SYN flood attack is when an attacker sends a series of SYN packets. Each packet causes the receiver to reply with a SYN-ACK response. The receiver then waits for the ACK that follows the SYN-ACK, and stores all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are only moved off the queue when an ACK comes back or when an internal timer ends the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for other users.

Figure 344 SYN Flood



30.8.2.4 LAND Attack

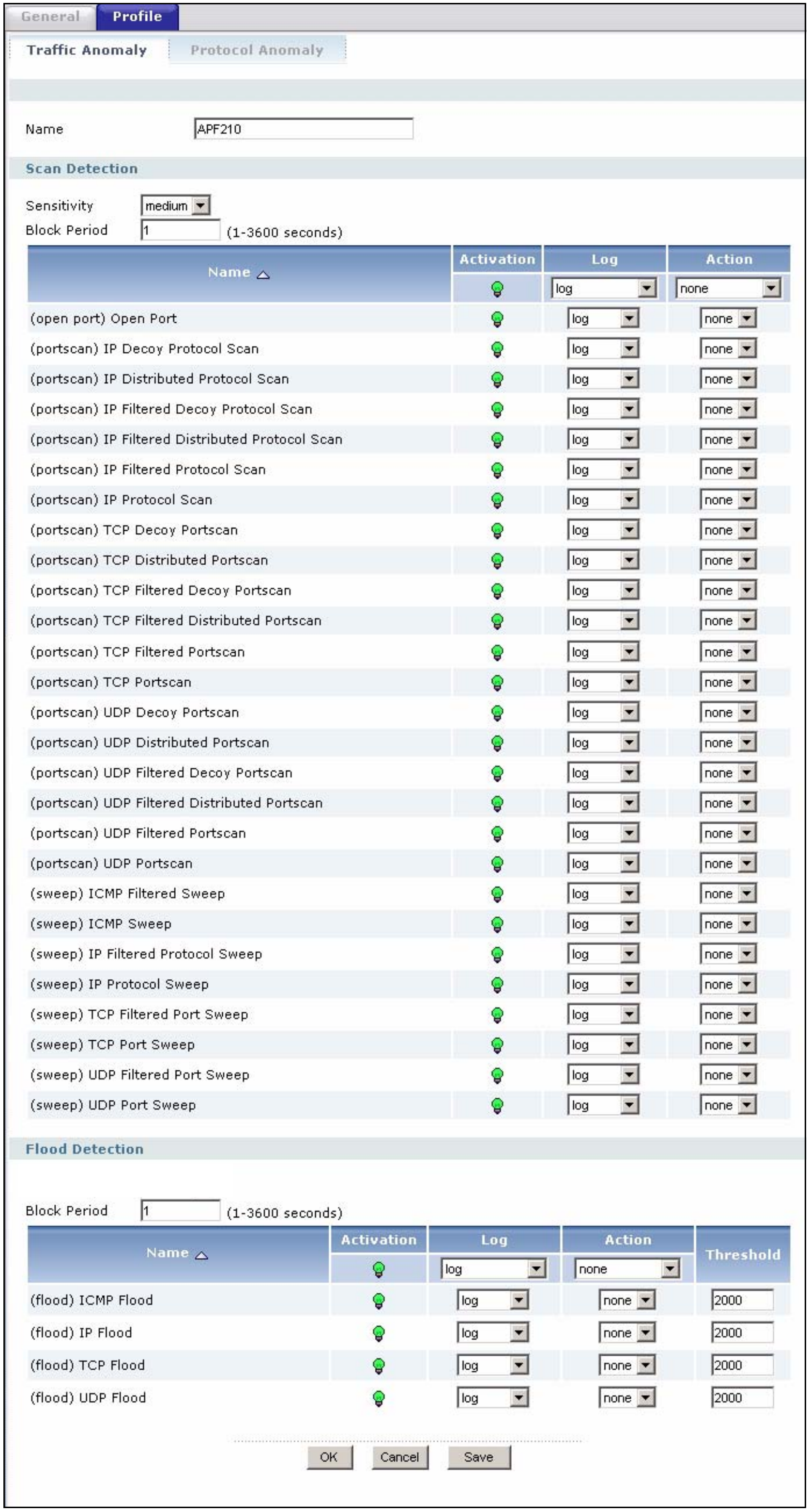
In a LAND attack, hackers flood SYN packets into a network with a spoofed source IP address of the network itself. This makes it appear as if the computers in the network sent the packets to themselves, so the network is unavailable while they try to respond to themselves.

30.8.2.5 UDP Flood Attack

UDP is a connection-less protocol and it does not require any connection setup procedure to transfer data. A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

30.8.3 Profile > Traffic Anomaly Screen

Figure 345 Profiles: Traffic Anomaly



Name: APF210

Scan Detection

Sensitivity: medium

Block Period: 1 (1-3600 seconds)

Name △	Activation	Log	Action
	●	log	none
(open port) Open Port	●	log	none
(portscan) IP Decoy Protocol Scan	●	log	none
(portscan) IP Distributed Protocol Scan	●	log	none
(portscan) IP Filtered Decoy Protocol Scan	●	log	none
(portscan) IP Filtered Distributed Protocol Scan	●	log	none
(portscan) IP Filtered Protocol Scan	●	log	none
(portscan) IP Protocol Scan	●	log	none
(portscan) TCP Decoy Portscan	●	log	none
(portscan) TCP Distributed Portscan	●	log	none
(portscan) TCP Filtered Decoy Portscan	●	log	none
(portscan) TCP Filtered Distributed Portscan	●	log	none
(portscan) TCP Filtered Portscan	●	log	none
(portscan) TCP Portscan	●	log	none
(portscan) UDP Decoy Portscan	●	log	none
(portscan) UDP Distributed Portscan	●	log	none
(portscan) UDP Filtered Decoy Portscan	●	log	none
(portscan) UDP Filtered Distributed Portscan	●	log	none
(portscan) UDP Filtered Portscan	●	log	none
(portscan) UDP Portscan	●	log	none
(sweep) ICMP Filtered Sweep	●	log	none
(sweep) ICMP Sweep	●	log	none
(sweep) IP Filtered Protocol Sweep	●	log	none
(sweep) IP Protocol Sweep	●	log	none
(sweep) TCP Filtered Port Sweep	●	log	none
(sweep) TCP Port Sweep	●	log	none
(sweep) UDP Filtered Port Sweep	●	log	none
(sweep) UDP Port Sweep	●	log	none

Flood Detection

Block Period: 1 (1-3600 seconds)

Name △	Activation	Log	Action	Threshold
	●	log	none	
(flood) ICMP Flood	●	log	none	2000
(flood) IP Flood	●	log	none	2000
(flood) TCP Flood	●	log	none	2000
(flood) UDP Flood	●	log	none	2000

The following table describes the fields in this screen.

Table 143 ADP > Profile > Traffic Anomaly

LABEL	DESCRIPTION
Name	This is the name of the ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: MyProfile mYProfile Mymy12_3-4 These are invalid profile names: 1mYProfile My Profile MyProfile? Whatalongprofilename123456789012
Scan/Flood Detection	
Sensitivity	(Scan detection only.) Select a sensitivity level so as to reduce false positives in your network. If you choose low sensitivity, then scan thresholds and sample times are set low, so you will have fewer logs and false positives; however some traffic anomaly attacks may not be detected. If you choose high sensitivity, then scan thresholds and sample times are set high, so most traffic anomaly attacks will be detected; however you will have more logs and false positives.
Block Period	Specify for how many seconds the ZyWALL blocks all packets from being sent to the victim (destination) of a detected anomaly attack.
Name	This is the name of the traffic anomaly rule. Click the **Name** column heading to sort in ascending or descending order according to the rule name.
Activation	Click the icon to enable or disable a rule or group of rules.
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 46 on page 625 for more on logs.
Action	Select what the ZyWALL should do when a packet matches a rule. **none**: The ZyWALL takes no action when a packet matches the signature(s). **block**: The ZyWALL silently drops packets that matches the rule. Neither sender nor receiver are notified.
Threshold	For flood detection you can set the number of detected flood packets per second that causes the ZyWALL to take the configured action.
OK	Click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the ZyWALL but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

30.9 Profiles: Protocol Anomaly

Protocol anomaly is the third screen in an ADP profile. Protocol anomaly (PA) rules check for protocol compliance against the relevant RFC (Request for Comments).

Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder where each category reflects the packet type inspected.

Protocol anomaly rules may be updated when you upload new firmware.

30.9.1 HTTP Inspection and TCP/UDP/ICMP Decoders

The following table gives some information on the HTTP inspection, TCP decoder, UDP decoder and ICMP decoder ZyWALL protocol anomaly rules.

Table 144 HTTP Inspection and TCP/UDP/ICMP Decoders

LABEL	DESCRIPTION
HTTP Inspection	
APACHE-WHITESPACE ATTACK	This rule deals with non-RFC standard of tab for a space delimiter. Apache uses this, so if you have an Apache server, you need to enable this option.
ASCII-ENCODING ATTACK	This rule can detect attacks where malicious attackers use ASCII-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
BARE-BYTE-UNICODING-ENCODING ATTACK	Bare byte encoding uses non-ASCII characters as valid values in decoding UTF-8 values. This is NOT in the HTTP standard, as all non-ASCII values have to be encoded with a %. Bare byte encoding allows the user to emulate an IIS server and interpret non-standard encodings correctly.
BASE36-ENCODING ATTACK	This is a rule to decode base36-encoded characters. This rule can detect attacks where malicious attackers use base36-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
DIRECTORY-TRAVERSAL ATTACK	This rule normalizes directory traversals and self-referential directories. So, “/abc/this_is_not_a_real_dir/../xyz” get normalized to “/abc/xyz”. Also, “/abc/./xyz” gets normalized to “/abc/xyz”. If a user wants to configure an alert, then specify “yes”, otherwise “no”. This alert may give false positives since some web sites refer to files using directory traversals.
DOUBLE-ENCODING ATTACK	This rule is IIS specific. IIS does two passes through the request URI, doing decodes in each one. In the first pass, IIS encoding (UTF-8 unicode, ASCII, bare byte, and %u) is done. In the second pass ASCII, bare byte, and %u encodings are done.
IIS-BACKSLASH-EVASION ATTACK	This is an IIS emulation rule that normalizes backslashes to slashes. Therefore, a request-URI of “/abc\xyz” gets normalized to “/abc/xyz”.
IIS-UNICODE-CODEPOINT-ENCODING ATTACK	This rule can detect attacks which send attack strings containing non-ASCII characters encoded by IIS Unicode. IIS Unicode encoding references the unicode.map file. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
MULTI-SLASH-ENCODING ATTACK	This rule normalizes multiple slashes in a row, so something like: “abc/////////xyz” get normalized to “abc/xyz”.
NON-RFC-DEFINED-CHAR ATTACK	This rule lets you receive a log or alert if certain non-RFC characters are used in a request URI. For instance, you may want to know if there are NULL bytes in the request-URI.
NON-RFC-HTTP-DELIMITER ATTACK	This is when a newline “\n” character is detected as a delimiter. This is non-standard but is accepted by both Apache and IIS web servers.

Table 144 HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

LABEL	DESCRIPTION
OVERSIZE-CHUNK-ENCODING ATTACK	This rule is an anomaly detector for abnormally large chunk sizes. This picks up the apache chunk encoding exploits and may also be triggered on HTTP tunneling that uses chunk encoding.
OVERSIZE-REQUEST-URI-DIRECTORY ATTACK	This rule takes a non-zero positive integer as an argument. The argument specifies the max character directory length for URL directory. If a URL directory is larger than this argument size, an alert is generated. A good argument value is 300 characters. This should limit the alerts to IDS evasion type attacks, like whisker.
SELF-DIRECTORY-TRAVERSAL ATTACK	This rule normalizes self-referential directories. So, “/abc/./xyz” gets normalized to “/abc/xyz”.
U-ENCODING ATTACK	This rule emulates the IIS %u encoding scheme. The %u encoding scheme starts with a %u followed by 4 characters, like %uXXXX. The XXXX is a hex encoded value that correlates to an IIS unicode codepoint. This is an ASCII value. An ASCII character is encoded like, %u002f = /, %u002e = ., etc.
UTF-8-ENCODING ATTACK	The UTF-8 decode rule decodes standard UTF-8 unicode sequences that are in the URI. This abides by the unicode standard and only uses % encoding. Apache uses this standard, so for any Apache servers, make sure you have this option turned on. When this rule is enabled, ASCII decoding is also enabled to enforce correct functioning.
WEBROOT-DIRECTORY-TRAVERSAL ATTACK	This is when a directory traversal traverses past the web server root directory. This generates much fewer false positives than the directory option, because it doesn’t alert on directory traversals that stay within the web server directory structure. It only alerts when the directory traversals go past the web server root directory, which is associated with certain web attacks.
TCP Decoder	
BAD-LENGTH-OPTIONS ATTACK	This is when a TCP packet is sent where the TCP option length field is not the same as what it actually is or is 0. This may cause some applications to crash.
EXPERIMENTAL-OPTIONS ATTACK	This is when a TCP packet is sent which contains non-RFC-complaint options. This may cause some applications to crash.
OBSOLETE-OPTIONS ATTACK	This is when a TCP packet is sent which contains obsolete RFC options.
OVERSIZE-OFFSET ATTACK	This is when a TCP packet is sent where the TCP data offset is larger than the payload.
TRUNCATED-OPTIONS ATTACK	This is when a TCP packet is sent which doesn’t have enough data to read. This could mean the packet was truncated.
TTCP-DETECTED ATTACK	T/TCP provides a way of bypassing the standard three-way handshake found in TCP, thus speeding up transactions. However, this could lead to unauthorized access to the system by spoofing connections.
UNDERSIZE-LEN ATTACK	This is when a TCP packet is sent which has a TCP datagram length of less than 20 bytes. This may cause some applications to crash.
UNDERSIZE-OFFSET ATTACK	This is when a TCP packet is sent which has a TCP header length of less than 20 bytes.This may cause some applications to crash.
UDP Decoder	
OVERSIZE-LEN ATTACK	This is when a UDP packet is sent which has a UDP length field of greater than the actual packet length. This may cause some applications to crash.

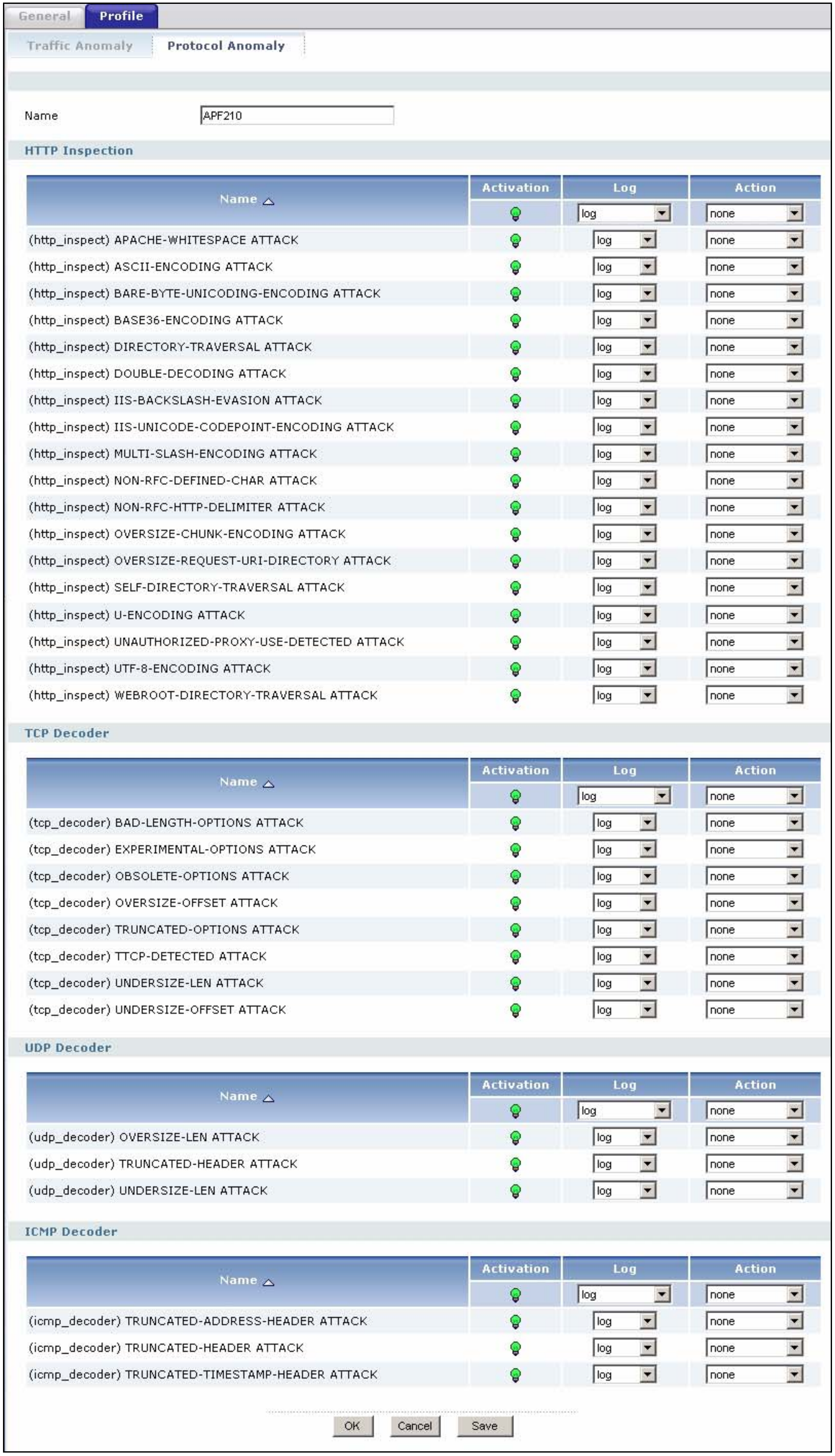
Table 144 HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

LABEL	DESCRIPTION
TRUNCATED-HEADER ATTACK	This is when a UDP packet is sent which has a UDP datagram length of less the UDP header length. This may cause some applications to crash.
UNDERSIZE-LEN ATTACK	This is when a UDP packet is sent which has a UDP length field of less than 8 bytes. This may cause some applications to crash.
ICMP Decoder	
TRUNCATED-ADDRESS-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP address header length. This may cause some applications to crash.
TRUNCATED-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP header length. This may cause some applications to crash.
TRUNCATED-TIMESTAMP-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP Time Stamp header length. This may cause some applications to crash.

30.9.2 Protocol Anomaly Configuration

In the **Anti-X > ADP > Profile** screen, click the **Edit** icon or click the **Add** icon and choose a base profile, then select the **Protocol Anomaly** tab. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Protocol Anomaly** tab.

Figure 346 Profiles: Protocol Anomaly



Name: APF210

HTTP Inspection

Name △	Activation	Log	Action
	●	log	none
(http_inspect) APACHE-WHITESPACE ATTACK	●	log	none
(http_inspect) ASCII-ENCODING ATTACK	●	log	none
(http_inspect) BARE-BYTE-UNICODING-ENCODING ATTACK	●	log	none
(http_inspect) BASE36-ENCODING ATTACK	●	log	none
(http_inspect) DIRECTORY-TRAVERSAL ATTACK	●	log	none
(http_inspect) DOUBLE-DECODING ATTACK	●	log	none
(http_inspect) IIS-BACKSLASH-EVASION ATTACK	●	log	none
(http_inspect) IIS-UNICODE-CODEPOINT-ENCODING ATTACK	●	log	none
(http_inspect) MULTI-SLASH-ENCODING ATTACK	●	log	none
(http_inspect) NON-RFC-DEFINED-CHAR ATTACK	●	log	none
(http_inspect) NON-RFC-HTTP-DELIMITER ATTACK	●	log	none
(http_inspect) OVERSIZE-CHUNK-ENCODING ATTACK	●	log	none
(http_inspect) OVERSIZE-REQUEST-URI-DIRECTORY ATTACK	●	log	none
(http_inspect) SELF-DIRECTORY-TRAVERSAL ATTACK	●	log	none
(http_inspect) U-ENCODING ATTACK	●	log	none
(http_inspect) UNAUTHORIZED-PROXY-USE-DETECTED ATTACK	●	log	none
(http_inspect) UTF-8-ENCODING ATTACK	●	log	none
(http_inspect) WEBROOT-DIRECTORY-TRAVERSAL ATTACK	●	log	none

TCP Decoder

Name △	Activation	Log	Action
	●	log	none
(tcp_decoder) BAD-LENGTH-OPTIONS ATTACK	●	log	none
(tcp_decoder) EXPERIMENTAL-OPTIONS ATTACK	●	log	none
(tcp_decoder) OBSOLETE-OPTIONS ATTACK	●	log	none
(tcp_decoder) OVERSIZE-OFFSET ATTACK	●	log	none
(tcp_decoder) TRUNCATED-OPTIONS ATTACK	●	log	none
(tcp_decoder) TTCP-DETECTED ATTACK	●	log	none
(tcp_decoder) UNDERSIZE-LEN ATTACK	●	log	none
(tcp_decoder) UNDERSIZE-OFFSET ATTACK	●	log	none

UDP Decoder

Name △	Activation	Log	Action
	●	log	none
(udp_decoder) OVERSIZE-LEN ATTACK	●	log	none
(udp_decoder) TRUNCATED-HEADER ATTACK	●	log	none
(udp_decoder) UNDERSIZE-LEN ATTACK	●	log	none

ICMP Decoder

Name △	Activation	Log	Action
	●	log	none
(icmp_decoder) TRUNCATED-ADDRESS-HEADER ATTACK	●	log	none
(icmp_decoder) TRUNCATED-HEADER ATTACK	●	log	none
(icmp_decoder) TRUNCATED-TIMESTAMP-HEADER ATTACK	●	log	none

The following table describes the fields in this screen.

Table 145 ADP > Profile > Protocol Anomaly

LABEL	DESCRIPTION
Name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: MyProfile mYProfile Mymy12_3-4 These are invalid profile names: 1mYProfile My Profile MyProfile? Whatalongprofilename123456789012
HTTP Inspection/TCP Decoder/UDP Decoder/ICMP Decoder	
Name	This is the name of the protocol anomaly rule. Click the **Name** column heading to sort in ascending or descending order according to the protocol anomaly rule name.
Activation	Click the icon to enable or disable a rule or group of rules.
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 46 on page 625 for more on logs.
Action	Select what the ZyWALL should do when a packet matches a rule. **none**: The ZyWALL takes no action when a packet matches the signature(s). **block**: The ZyWALL silently drops packets that matches the rule. Neither sender nor receiver are notified.
OK	Click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the ZyWALL but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

31

Content Filter Screens

This chapter covers how to use the content filter feature to control web access. See Section 5.4.17 on page 120 for related information on these screens.

31.1 Content Filter Overview

Content filter allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users or groups and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

31.1.1 Content Filter Policies

A content filter policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

31.1.2 Content Filter Profiles

A content filter profile conveniently stores your custom settings for the following features.

31.1.2.1 Category-based Blocking

The ZyWALL can block access to particular categories of web site content, such as pornography or racial intolerance.

31.1.2.2 Restrict Web Features

The ZyWALL can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

31.1.2.3 Customize Web Site Access

You can specify URLs to which the ZyWALL blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the ZyWALL block access to URLs that contain particular keywords.

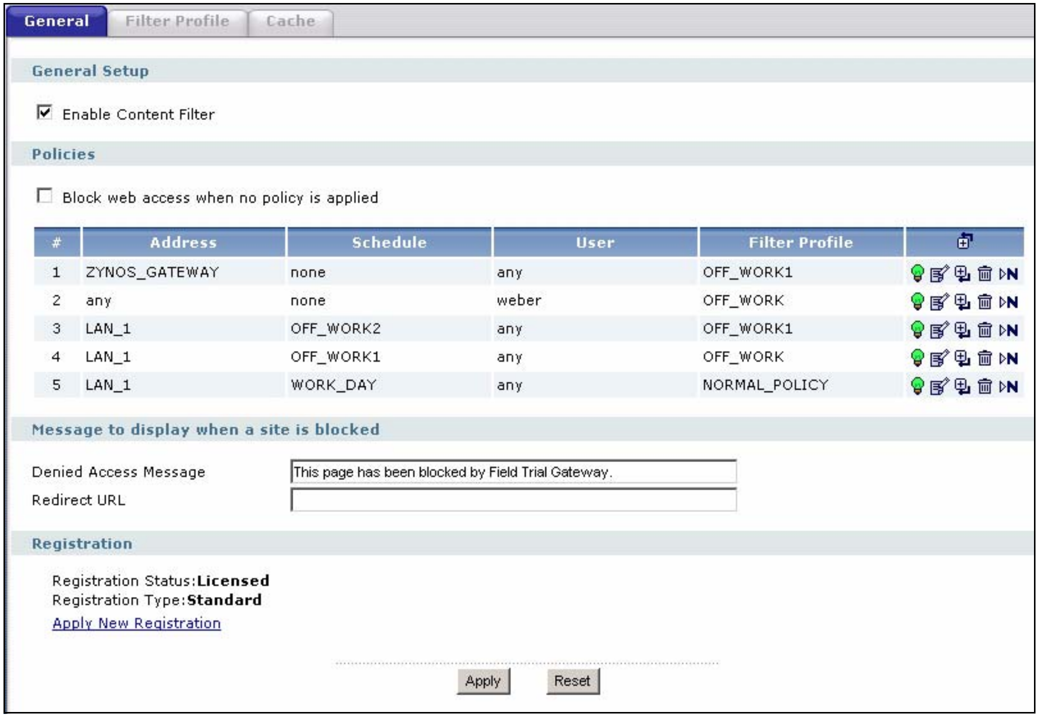
31.1.3 Content Filter Configuration Guidelines

You must configure an address object, a schedule object and a filtering profile before you can set up a content filter policy. When the ZyWALL receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The ZyWALL allows the request if the default policy is not set to block. The ZyWALL blocks the request if the default policy is set to block.

31.2 Content Filter General Screen

Click **Anti-X** > **Content Filter** > **General** to open the **Content Filter General** screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Figure 347 Anti-X > Content Filter > General



General Setup

☑ Enable Content Filter

Policies

☐ Block web access when no policy is applied

#	Address	Schedule	User	Filter Profile
1	ZYNOS_GATEWAY	none	any	OFF_WORK1
2	any	none	weber	OFF_WORK
3	LAN_1	OFF_WORK2	any	OFF_WORK1
4	LAN_1	OFF_WORK1	any	OFF_WORK
5	LAN_1	WORK_DAY	any	NORMAL_POLICY

Message to display when a site is blocked

Denied Access Message: This page has been blocked by Field Trial Gateway.
Redirect URL:

Registration

Registration Status:**Licensed**
Registration Type:**Standard**
Apply New Registration

The following table describes the labels in this screen.

Table 146 Anti-X > Content Filter > General

LABEL	DESCRIPTION
General Setup	
Enable Content Filter	Select this check box to enable the content filter.
Policies	This is a list of the configured content filter policies.

Table 146 Anti-X > Content Filter > General (continued)

LABEL	DESCRIPTION
Block web access when no policy is applied	Select this check box to stop users from accessing the Internet by default when their attempted access does not match a content filter policy.
#	This column lists the index numbers of the content filter policies.
Address	A content filter policy applies to web access from the IP addresses listed here. **any** means the content filter policy applies to all of the web access requests that the ZyWALL receives from any IP address.
Schedule	This column displays the name of the schedule for each content filter policy. You can define different policies for different time periods. **none** means the content filter policy applies all of the time.
User	This column displays the individual or group to which this policy applies. **any** means the content filter policy applies to all of the web access requests that the ZyWALL receives from any user.
Filter Profile	This column displays the name of the content filter profile that each content filter policy uses. The content filter profile defines to which web services, web sites or web site categories access is to be allowed or denied.
Add	Click the **Add** icon at the top of the column to create a new content filter policy at the top of the list. The **Active** icon shows the entry is enabled. Click this icon to disable the entry. The **Inactive** icon shows the entry is disabled. Click this icon to enable the entry. Click the **Edit** icon to go to a screen where you can change the configuration settings of an entry. Click the **Remove** icon to delete an entry from the list. Click the **Move to N** icon, type a number in the move entry dialog box and press [ENTER] to move the entry to the numbered location. Click a content filter policy's **Add** icon to create a new content filter policy above the current line. All other entries below the new entry are pushed down. The ordering of the content filter policies is important as they are used in the order they are listed. The ZyWALL checks requests for Web sessions against the list of content filter policies (starting from the first in the list). The ZyWALL's content filter feature blocks or allows the Web session according to the first matching content filter policy and does not check any other content filter policies. The ZyWALL does not perform content filter on Web session requests that do not match any of the content filter policies.
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,). For example, "Access to this web page is not allowed. Please contact the network administrator".
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.

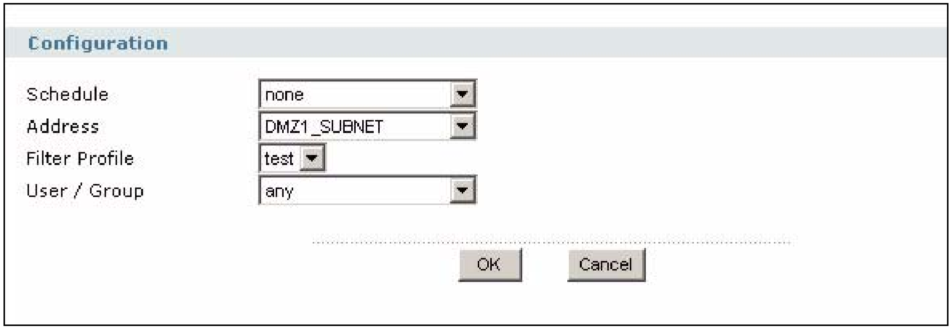
Table 146 Anti-X > Content Filter > General (continued)

LABEL	DESCRIPTION
Registration Status	This read-only field displays the status of your content-filtering database service registration. **Not Licensed** displays if you have not successfully registered and activated the service. **Expired** displays if your subscription to the service has expired. **Licensed** displays if you have successfully registered the ZyWALL and activated the service. After you register for content filter, you can see Chapter 31 on page 469 for how to use the **Test Against Web Filtering Server** button. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. You can view content filter reports after you register the ZyWALL and activate the subscription service in the **Registration** screen (see Chapter 32 on page 483).
Registration Type	This read-only field displays what kind of service registration you have for the content-filtering database. **None** displays if you have not successfully registered and activated the service. **Standard** displays if you have successfully registered the ZyWALL and activated the service. **Trial** displays if you have successfully registered the ZyWALL and activated the trial service subscription.
Apply new Registration	This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

31.3 Content Filter Policy Screen

Click **Anti-X** > **Content Filter** > **General** > **Add** or **Edit** to open the **Content Filter Policy** screen. Use this screen to configure a content filter policy. A content filter policy defines which content filter profile should be applied, when it should be applied, and to whose web access it should be applied.

Figure 348 Anti-X > Content Filter > General > Add I



Configuration

Schedule: none

Address: DMZ1_SUBNET

Filter Profile: test

User / Group: any

The following table describes the labels in this screen.

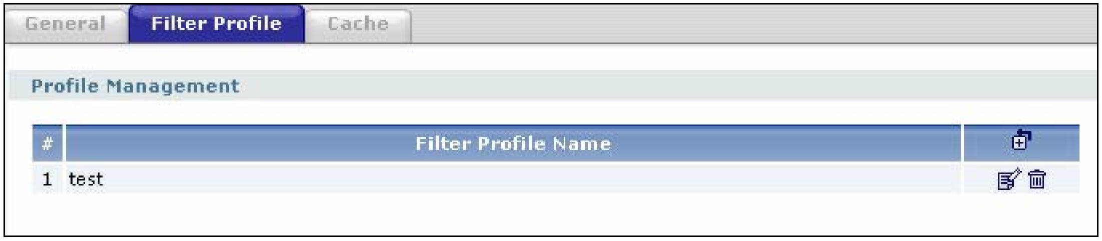
Table 147 Anti-X > Content Filter > General > Add

LABEL	DESCRIPTION
Schedule	Select a schedule to define when to apply this content filter policy. You can define different policies for different time periods. For example, you could have one policy that blocks access to certain categories of web sites during working hours and another policy that allows access to certain categories after the work day is over. Select **Create Object** to configure a new schedule (see Chapter 37 on page 527 for details). Select **none** to have the content filter policy apply all of the time.
Address	Select the address or address group for which you wan to use this policy. Select **Create Object** to configure a new address or address group. Select **any** to have the content filter policy apply to all of the web access requests that the ZyWALL receives from any IP address.
Filter Profile	Use the drop-down list box to select the content filter profile that you want to use for this policy. The content filter profile defines to which web services, web sites or web site categories access is to be allowed or denied. Use the content filter **Filter Profile** screens to configure the profiles.
User/Group	Use the drop-down list box to select the individual or group for which you want to use this policy. Select **Create Object** to configure a new user account (see Section 34.2.1 on page 506 for details). Select **any** to have the content filter policy apply to all of the web access requests that the ZyWALL receives from any user.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

31.4 Content Filter Profile Screen

Click **Anti-X** > **Content Filter** > **Filter Profile** to open the **Filter Profile** screen. A content filter profile defines to which web services, web sites or web site categories access is to be allowed or denied.

Figure 349 Anti-X > Content Filter > Filter Profile



#	Filter Profile Name
1	test

The following table describes the labels in this screen.

Table 148 Anti-X > Content Filter > Filter Profile

LABEL	DESCRIPTION
#	This column lists the index numbers of the content filter profiles.
Filtering Profile Name	This column lists the names of the content filter profiles.

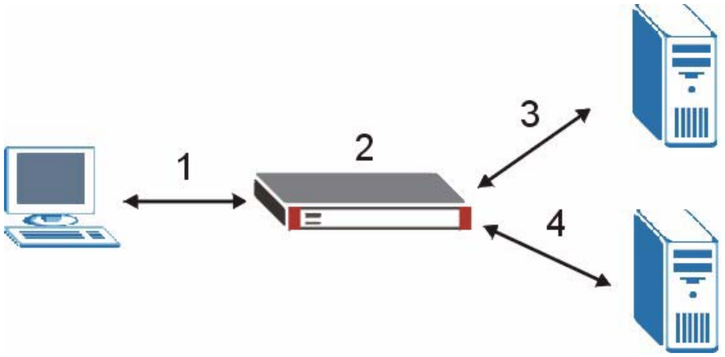
Table 148 Anti-X > Content Filter > Filter Profile (continued)

LABEL	DESCRIPTION
Add	Click the **Add** icon at the top of the column to create a new content filter profile at the end of the list. Click a content filter policy's **Add** icon at the to create a new content filter policy below the current line. All other entries below the new entry are pushed down.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

31.5 External Web Filtering Service

When you register for and enable the external web filtering service, your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories. The content filter lookup process is described below.

Figure 350 Content Filter Lookup Procedure



1 A computer behind the ZyWALL tries to access a web site.

2 The ZyWALL looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the ZyWALL's cache. The ZyWALL blocks, blocks and logs or just logs the request based on your configuration.

3 Use the **Content Filter Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses (see Section 31.9 on page 480). All of the web site address records are also cleared from the local cache when the ZyWALL restarts.

4 If the ZyWALL has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.

5 The external content filter server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the ZyWALL's content filter cache.

31.6 Content Filter Categories Screen

Click **Anti-X** > **Content Filter** > **Filter Profile** > **Add** or **Edit** to open the **Categories** screen. Use this screen to enable external database content filtering and select which web site categories to block and/or log.

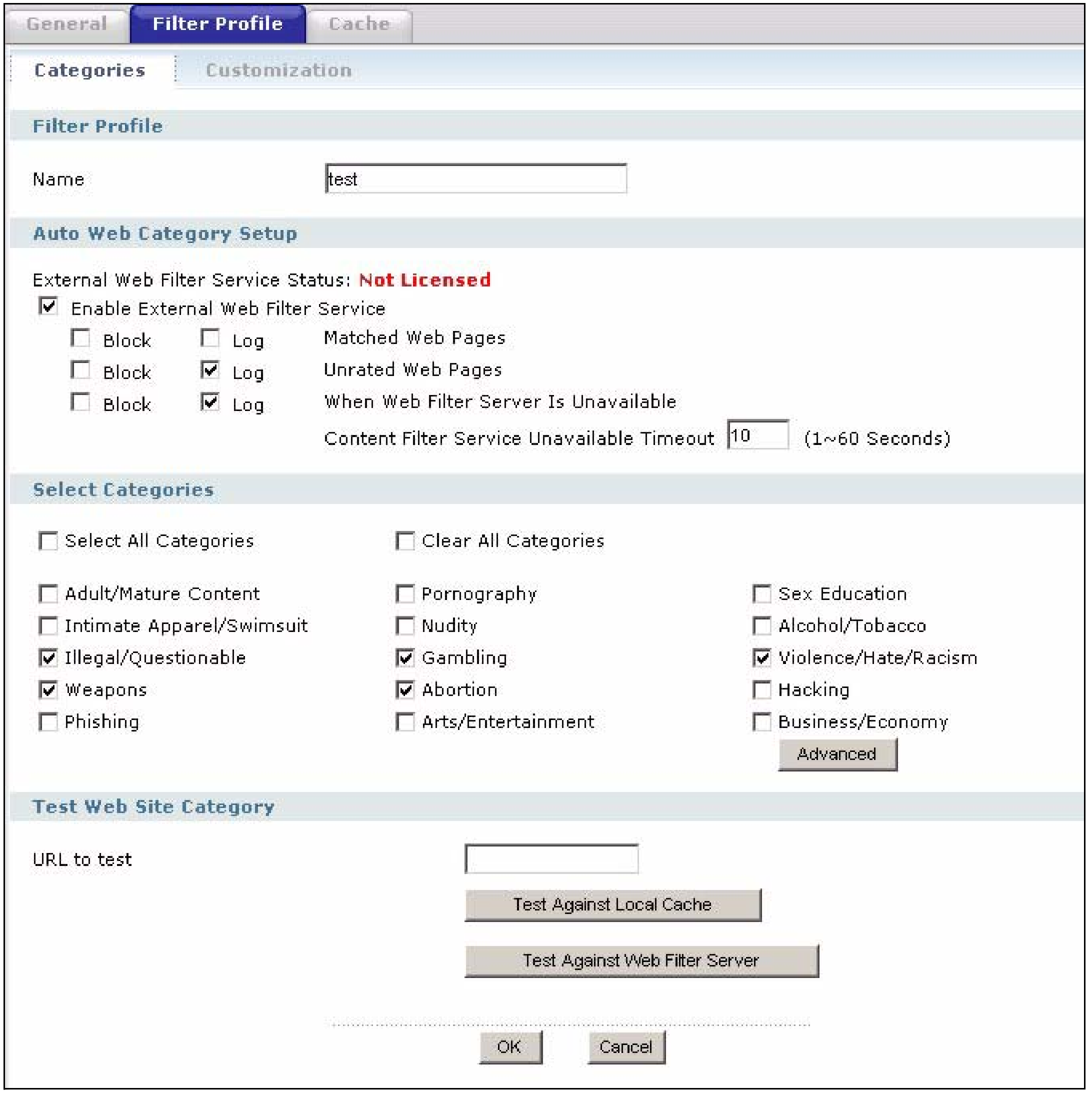
You must register for external content filtering before you can use it.

See Section 8.2 on page 166 for how to register.

Do the following to view content filtering reports (see Chapter 32 on page 483 for details).

1. Log into myZyXEL.com and click your device’s link to open it’s **Service Management** screen.
2. Click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.
3. Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen (Figure 356 on page 484). Type your myZyXEL.com account password in the **Password** field. Click **Submit**.

Figure 351 Anti-X > Content Filter > Filter Profile > Add



General
Filter Profile
Cache
Categories
Customization

Filter Profile

Name: test

Auto Web Category Setup

External Web Filter Service Status: Not Licensed

☑ Enable External Web Filter Service

☐ Block ☐ Log Matched Web Pages

☐ Block ☑ Log Unrated Web Pages

☐ Block ☑ Log When Web Filter Server Is Unavailable

Content Filter Service Unavailable Timeout 10 (1~60 Seconds)

Select Categories

☐ Select All Categories ☐ Clear All Categories

☐ Adult/Mature Content	☐ Pornography	☐ Sex Education
☐ Intimate Apparel/Swimsuit	☐ Nudity	☐ Alcohol/Tobacco
☑ Illegal/Questionable	☑ Gambling	☑ Violence/Hate/Racism
☑ Weapons	☑ Abortion	☐ Hacking
☐ Phishing	☐ Arts/Entertainment	☐ Business/Economy

Advanced
Test Web Site Category
URL to test
Test Against Local Cache
Test Against Web Filter Server
OK
Cancel

The following table describes the labels in this screen.

Table 149 Anti-X > Content Filter > Filter Profile > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Auto Web Category Setup	
External Web Filter Service Status	This read-only field displays the status of your external content filtering service registration. **Not Licensed** displays if you have not successfully registered and activated the service. **Expired** displays if your subscription to the service has expired. **Licensed** displays if you have successfully registered the ZyWALL and activated the service.

Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Enable External Web Filter Service	Enable external database content filtering to have the ZyWALL check an external database to find to which category a requested web page belongs. The ZyWALL then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Matched Web Pages	Select **Block** to prevent users from accessing web pages that match the categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page. Select **Log** to record attempts to access prohibited web pages.
Unrated Web Pages	Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page. Select **Log** to record attempts to access web pages that are not categorized.
When Web Filter Server Is Unavailable	Select **Block** to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes: There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field. The ZyWALL is not able to resolve the domain name of the external content filtering database. There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid"). Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable.
Content Filter Service Unavailable Timeout	Specify a number of seconds (1 to 60) for the ZyWALL to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the ZyWALL blocks or allows access to the requested web page based on the setting in the **Block When Content Filter Server Is Unavailable** field. This setting applies to all of your content filtering profiles.
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Adult/Mature Content	Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children.
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement.

Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Intimate Apparel/Swimsuit	Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered.
Nudity	Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals.
Alcohol/Tobacco	Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products.
Illegal/Questionable	Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers. Note: This category includes sites identified as being malicious in any way (such as having viruses, spyware and etc.).
Gambling	Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements).
Violence/Hate/Racism	Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics.
Weapons	Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use.
Abortion	Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Hacking	Selecting this category excludes pages that distribute, promote, or provide hacking tools and/or information which may help gain unauthorized access to computer systems and/or computerized communication systems. Hacking encompasses instructions on illegal or questionable tactics, such as creating viruses, distributing cracked or pirated software, or distributing other protected intellectual property.
Phishing	Selecting this category excludes pages that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (i.e. credit card numbers, pin numbers).

Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Arts/Entertainment	Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment.
Business/Economy	Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services).
Alternative Spirituality/ Occult	Selecting this category excludes pages that promote and provide information on religions such as Wicca, Witchcraft or Satanism. Occult practices, atheistic views, voodoo rituals or any other form of mysticism are represented here. Includes sites that endorse or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, incantations, curses and magic powers. This category includes sites which discuss or deal with paranormal or unexplained events.
Illegal Drugs	Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Education	Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups.
Cultural/Charitable Organization	Selecting this category excludes pages that nurture cultural understanding and foster volunteerism such as 4H, the Lions and Rotary Clubs. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Sites that provide a learning environment or cultural refinement/awareness outside of the strictures of formalized education such as museums and planetariums are included under this heading.
Financial Services	Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services.
Brokerage/Trading	Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news.
Online Games	Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways.
Government/Legal	Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities.
Military	Selecting this category excludes pages that promote or provide information on military branches or armed services.

Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Political/Activist Groups	Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities.
Health	Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition.
Computers/Internet	Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies.
Search Engines/Portals	Selecting this category excludes pages that support searching the Internet, indices, and directories.
Spyware/Malware Sources	Selecting this category excludes pages which distribute spyware and other malware. Spyware is defined as software which takes control of your computer, modifies computer settings, collects or reports personal information, or misrepresents itself by tricking users to install, download, or enter personal information. This includes drive-by downloads; browser hijackers; dialers; intrusive advertising; any program which modifies your homepage, bookmarks, or security settings; and keyloggers. It also includes any software which bundles spyware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as e-mail addresses, name, social security number, IP address, etc. A site is not classified as spyware if the user is reasonably notified that the software will perform these actions (that is, it alerts that it will send personal information, be installed, or that it will log keystrokes). Note: Sites rated as spyware should have a second category assigned with them.
Spyware Effects/Privacy Concerns	Selecting this category excludes pages to which spyware (as defined in the Spyware/Malware Sources category) reports its findings or from which it alone downloads advertisements. Also includes sites that contain serious privacy issues, such as “phone home” sites to which software can connect and send user info; sites that make extensive use of tracking cookies without a posted privacy statement; and sites to which browser hijackers redirect users. Usually does not include sites that can be marked as Spyware/Malware. Note: Sites rated as spyware effects typically have a second category assigned with them.
Job Search/Careers	Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers.
News/Media	Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories.
Personals/Dating	Selecting this category excludes pages that promote interpersonal relationships.
Reference	Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information.

Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Open Image/Media Search	Selecting this category excludes pages with image or video search capabilities which return graphical results (i.e. thumbnail pictures) that include potentially pornographic content along with non-pornographic content (as defined in the Pornography category). Sites that explicitly exclude offensive content are not included in this category.
Chat/Instant Messaging	Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads.
Email	Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services.
Blogs/Newsgroups	Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems. Also, blog specific sites or an individual with his own blog. This does not include social networking communities with blogs.
Religion	Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft or atheist beliefs (Alternative Spirituality/Occult).
Social Networking	Selecting this category excludes pages that enable people to connect with others to form an online community. Typically members describe themselves in personal web page profiles and form interactive networks, linking them with other members based on common interests or acquaintances. Instant messaging, file sharing and web logs (blogs) are common features of Social Networking sites. Note: These sites may contain offensive material in the community-created content. Sites in this category are also referred to as "virtual communities" or "online communities". This category does not include more narrowly focused sites, like those that specifically match descriptions for Personals/Dating sites or Business sites.
Online Storage	Selecting this category excludes pages that provide a secure, encrypted, off-site backup and restoration of personal data. These online repositories are typically used to store, organize and share videos, music, movies, photos, documents and other electronically formatted information. Sites that fit this criteria essentially act as your personal hard drive on the Internet.
Remote Access Tools	Selecting this category excludes pages that primarily focus on providing information about and/or methods that enables authorized access to and use of a desktop computer or private network remotely.
Shopping	Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons).
Auctions	Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements.
Real Estate	Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties.
Society/Lifestyle	Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category.

Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Sexuality/Alternative Lifestyles	Selecting this category excludes pages that provide information, promote, or cater to gays, lesbians, swingers, other sexual orientations or practices, or a particular fetish. This category does not include sites that are sexually gratuitous in nature which would typically fall under the Pornography category.
Restaurants/Dining/Food	Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes.
Sports/Recreation/Hobbies	Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting.
Travel	Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
Vehicles	Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts.
Humor/Jokes	Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating.
Software Downloads	Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge.
Pay to Surf	Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
Peer-to-Peer	Selecting this category excludes pages that distribute software to facilitate the direct exchange of files between users, including software that enables file search and sharing across a network without dependence on a central server.
Streaming Media/MP3s	Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers.
Proxy Avoidance	Selecting this category excludes pages that provide information on how to bypass proxy server/appliance features or gain access to URLs in any way that bypasses the proxy server/appliance.
For Kids	Selecting this category excludes pages designed specifically for children.
Web Advertisements	Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.
Web Hosting	Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services.
Advanced/Basic	Click **Advanced** to see an expanded list of categories, or click **Basic** to see a smaller list.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box.

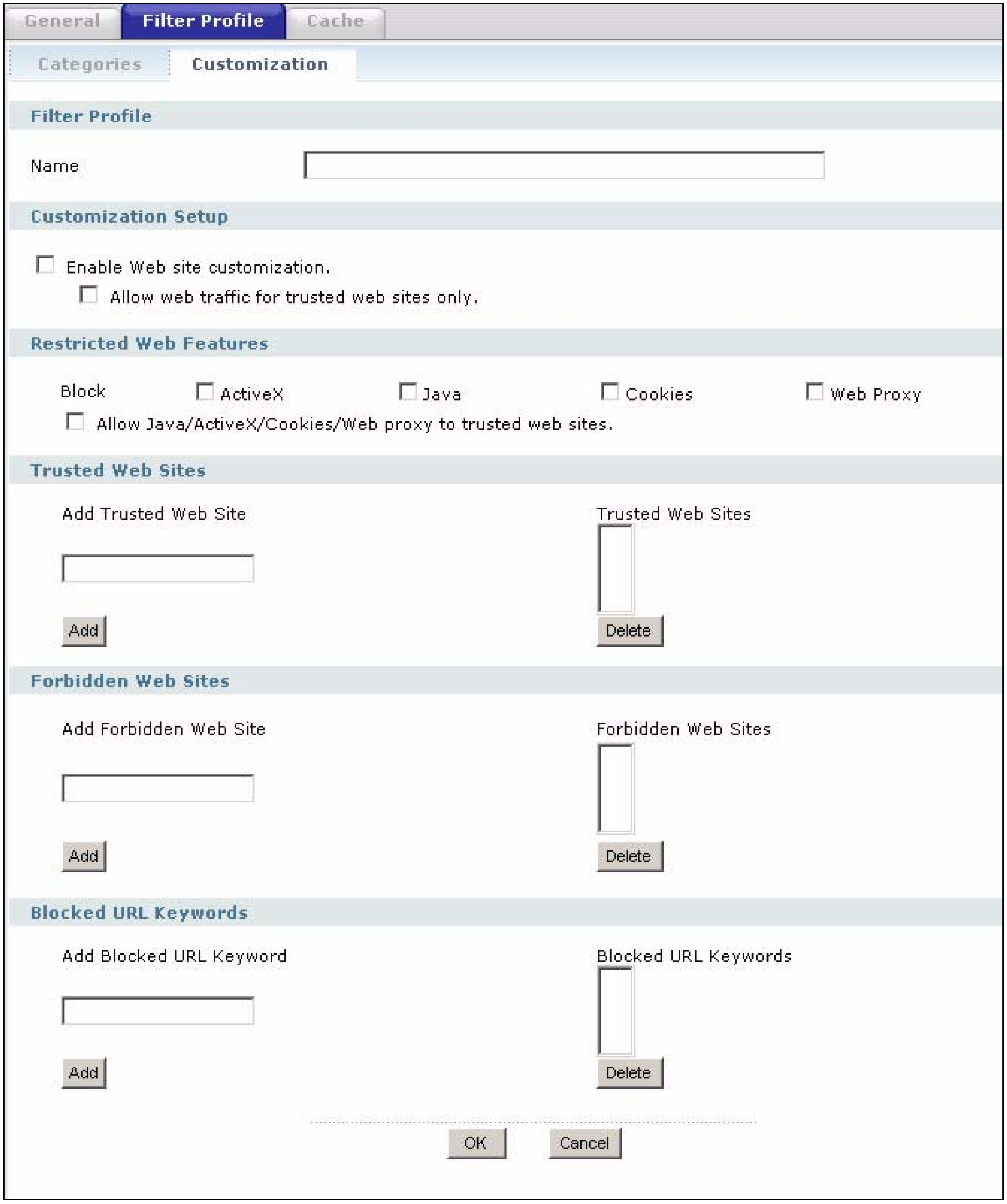
Table 149 Anti-X > Content Filter > Filter Profile > Add (continued)

LABEL	DESCRIPTION
Test Against Local Cache	Click this button to see the category recorded in the ZyWALL's content filtering database for the web page you specified (if the database has an entry for it).
Test Against Web Filter Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

31.7 Content Filter Customization Screen

Click **Anti-X** > **Content Filter** > **Filter Profile** > **Add** or **Edit** > **Customization** to open the **Customization** screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Figure 352 Anti-X > Content Filter > Filter Profile > Customization


General
Filter Profile
Cache
Categories
Customization
Filter Profile
Name
Customization Setup
☐ Enable Web site customization.
☐ Allow web traffic for trusted web sites only.
Restricted Web Features
Block
☐ ActiveX
☐ Java
☐ Cookies
☐ Web Proxy
☐ Allow Java/ActiveX/Cookies/Web proxy to trusted web sites.
Trusted Web Sites
Add Trusted Web Site
Add
Trusted Web Sites
Delete
Forbidden Web Sites
Add Forbidden Web Site
Add
Forbidden Web Sites
Delete
Blocked URL Keywords
Add Blocked URL Keyword
Add
Blocked URL Keywords
Delete
OK
Cancel

The following table describes the labels in this screen.

Table 150 Anti-X > Content Filter > Filter Profile > Customization

LABEL	DESCRIPTION
Filter Profile	
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Customization Setup	
Enable Web site customization	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.

Table 150 Anti-X > Content Filter > Filter Profile > Customization (continued)

LABEL	DESCRIPTION
Allow Web traffic for trusted web sites only	When this box is selected, the ZyWALL blocks Web access to sites that are not on the **Trusted Web Sites** list. If they are chosen carefully, this is the most effective way to block objectionable material.
Restricted Web Features	Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Cookies are files stored on a computer’s hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Allow Java/ActiveX/Cookies/Web proxy to trusted web sites	When this box is selected, the ZyWALL will permit Java, ActiveX and Cookies from sites on the **Trusted Web Sites** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 256 entries.
Add Trusted Web Site	Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc. Use up to 63 characters (0-9a-z-). The casing does not matter.
Trusted Web Sites	This list displays the trusted web sites already added.
Add	Click this button when you have finished adding the host name in the text field above.
Delete	Select a web site name from the **Trusted Web Sites** list, and then click this button to delete it from that list.
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 256 entries.
Add Forbidden Web Site	Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are also blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. Use up to 63 characters (0-9a-z-). The casing does not matter.
Forbidden Web Sites	This list displays the forbidden web sites already added.
Add	Click this button when you have finished adding the host name in the text field above.
Delete	Select a web site name from the **Forbidden Web Sites** list, and then click this button to delete it from that list.

Table 150 Anti-X > Content Filter > Filter Profile > Customization (continued)

LABEL	DESCRIPTION
Blocked URL Keywords	This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address.
Add Blocked URL Keyword	Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,). For example enter Bad_Site to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).
Blocked URL Keywords	This list displays the keywords already added.
Add	Click this button when you have finished adding the key words field above.
Delete	Select a keyword from the **Blocked URL Keywords** list, and then click this button to delete it from that list.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

31.8 Keyword Blocking URL Checking

The ZyWALL checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the ZyWALL checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the ZyWALL would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

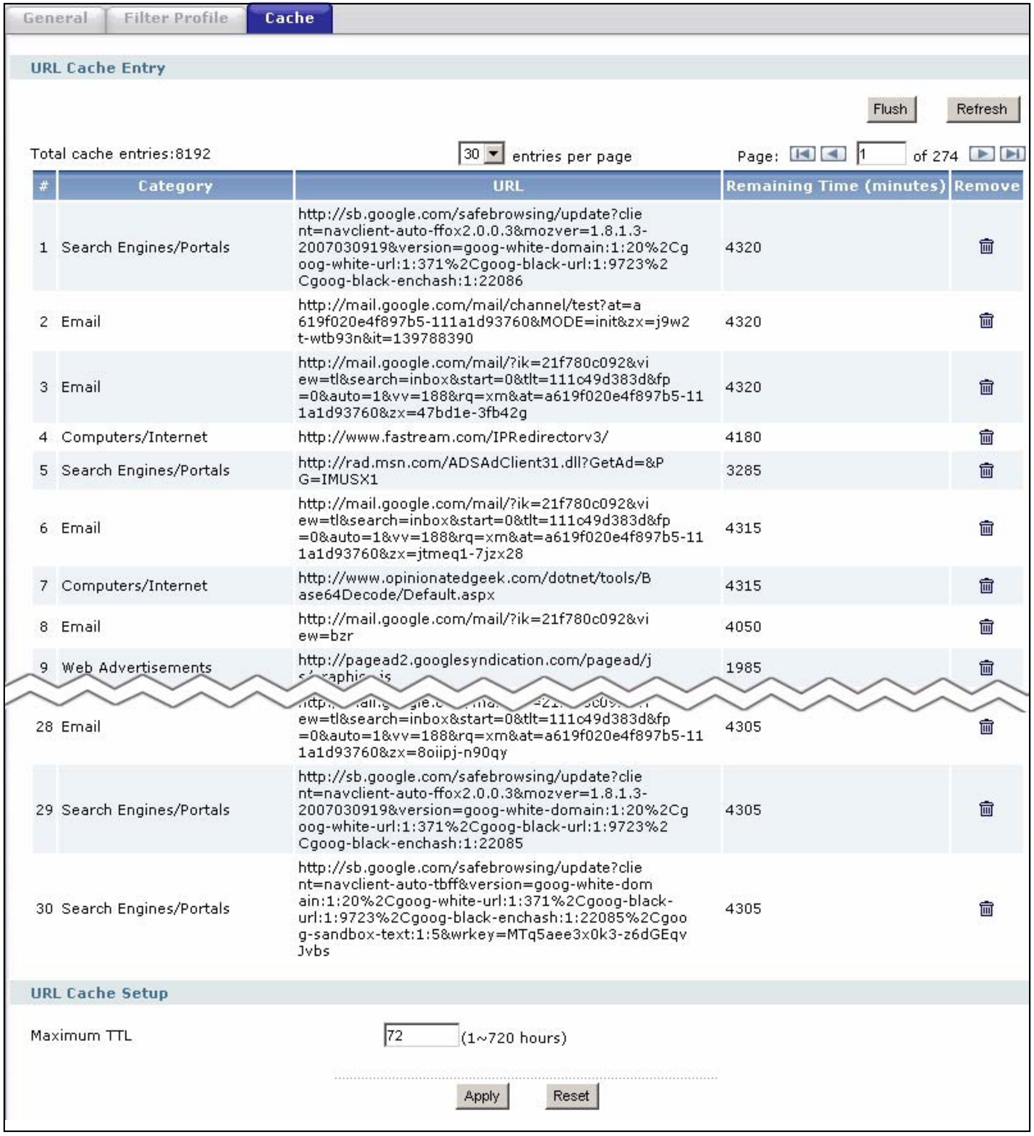
31.9 Content Filter Cache Screen

Click **Anti-X > Content Filter > Cache** to display the **Content Filter Cache** screen. Use this screen to view and configure your ZyWALL's URL caching. You can also configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The ZyWALL only queries the external content filtering database for sites not found in the cache.

You can remove individual entries from the cache. When you do this, the ZyWALL queries the external content filtering database the next time someone tries to access that web site. This allows you to check whether a web site's category has been changed.

Please see Section 32.2 on page 488 for how to submit a web site that has been incorrectly categorized.

Figure 353 Anti-X > Content Filter > Cache



Total cache entries:8192

30 entries per page

Page: 1 of 274

#	Category	URL	Remaining Time (minutes)	Remove
1	Search Engines/Portals	http://sb.google.com/safebrowsing/update?client=navclient-auto-ffox2.0.0.3&mozver=1.8.1.3-2007030919&version=goog-white-domain:1:20%2Cgoog-white-url:1:371%2Cgoog-black-url:1:9723%2Cgoog-black-enchash:1:22086	4320	🗑
2	Email	http://mail.google.com/mail/channel/test?at=a619f020e4f897b5-111a1d93760&MODE=init&zx=j9w2t-wtb93n&it=139788390	4320	🗑
3	Email	http://mail.google.com/mail/?ik=21f780c092&view=tl&search=inbox&start=0&tlt=111c49d383d&fp=0&auto=1&vv=188&rq=xm&at=a619f020e4f897b5-111a1d93760&zx=47bd1e-3fb42g	4320	🗑
4	Computers/Internet	http://www.fastream.com/IPRedirectorv3/	4180	🗑
5	Search Engines/Portals	http://rad.msn.com/ADSAdClient31.dll?GetAd=&PG=IMUSX1	3285	🗑
6	Email	http://mail.google.com/mail/?ik=21f780c092&view=tl&search=inbox&start=0&tlt=111c49d383d&fp=0&auto=1&vv=188&rq=xm&at=a619f020e4f897b5-111a1d93760&zx=jtmeq1-7jzx28	4315	🗑
7	Computers/Internet	http://www.opinionatedgeek.com/dotnet/tools/Base64Decode/Default.aspx	4315	🗑
8	Email	http://mail.google.com/mail/?ik=21f780c092&view=bzr	4050	🗑
9	Web Advertisements	http://pagead2.googlesyndication.com/pagead/j	1985	🗑
28	Email	ew=tl&search=inbox&start=0&tlt=111c49d383d&fp=0&auto=1&vv=188&rq=xm&at=a619f020e4f897b5-111a1d93760&zx=8oiipj-n90qy	4305	🗑
29	Search Engines/Portals	http://sb.google.com/safebrowsing/update?client=navclient-auto-ffox2.0.0.3&mozver=1.8.1.3-2007030919&version=goog-white-domain:1:20%2Cgoog-white-url:1:371%2Cgoog-black-url:1:9723%2Cgoog-black-enchash:1:22085	4305	🗑
30	Search Engines/Portals	http://sb.google.com/safebrowsing/update?client=navclient-auto-tbff&version=goog-white-domain:1:20%2Cgoog-white-url:1:371%2Cgoog-black-url:1:9723%2Cgoog-black-enchash:1:22085%2Cgoog-sandbox-text:1:5&wrkey=MTq5aee3x0k3-z6dGEqvJvbs	4305	🗑

Maximum TTL 72 (1~720 hours)

The following table describes the labels in this screen.

Table 151 Anti-X > Content Filter > Cache

LABEL	DESCRIPTION
URL Cache Entry	
Flush	Click this button to clear all web site addresses from the cache manually.
Refresh	Click this button to reload the list of content filter cache entries.
Total cache entries	This is the number of web site addresses in the content filter cache.
entries per page	Select how many web site addresses to display per page in the screen.

Table 151 Anti-X > Content Filter > Cache (continued)

LABEL	DESCRIPTION
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This is the index number of a categorized web site address record.
Category	This field shows whether access to the web site's URL was blocked-or allowed. Click the column heading to sort the entries. Point the triangle up to display the blocked URLs before the URLs to which access was allowed. Point the triangle down to display the URLs to which access was allowed before the blocked URLs.
URL	This is a web site's address that the ZyWALL previously checked with the external content filtering database.
Remaining Time (minutes)	This is the number of minutes left before the URL entry is discarded from the cache.
Remove	Click the **Delete** icon to remove the URL entry from the cache.
URL Cache Setup	
Maximum TTL	Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the ZyWALL is to keep an entry in the URL cache before discarding it. The external content filtering database frequently adds previously uncategorized web sites and sometimes changes a web site's category. Setting this limit higher will speed up the processing of web access requests but will also make it take longer for the ZyWALL to reflect changes in the external content filtering database.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

32

Content Filter Reports

This chapter describes how to view content filtering reports after you have activated the category-based content filtering subscription service.

See Chapter 8 on page 165 on how to create a myZyXEL.com account, register your device and activate the subscription services.

32.1 Viewing Content Filter Reports

Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

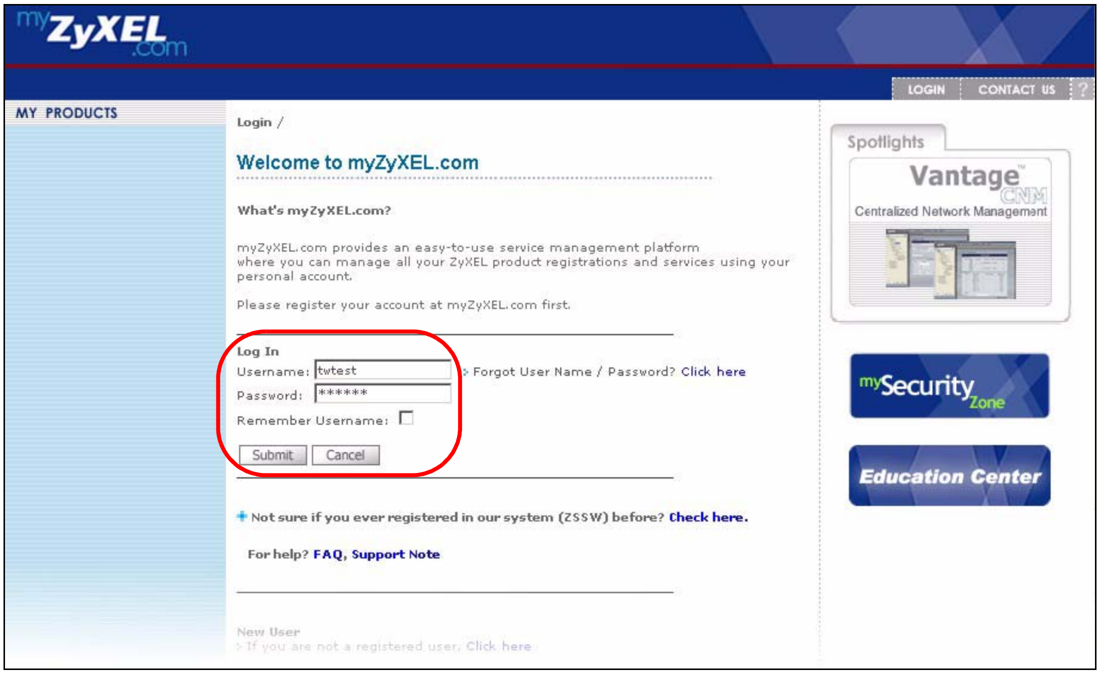
You need to register your iCard before you can view content filtering reports.

Alternatively, you can also view content filtering reports during the free trial (up to 30 days).

1 Go to http://www.myZyXEL.com.

2 Fill in your myZyXEL.com account information and click **Submit**.

Figure 354 myZyXEL.com: Login



Welcome to myZyXEL.com

What's myZyXEL.com?

myZyXEL.com provides an easy-to-use service management platform where you can manage all your ZyXEL product registrations and services using your personal account.

Please register your account at myZyXEL.com first.

Log In

Username: twtest

Password: ******

Remember Username: ☐

> Forgot User Name / Password? Click here

Not sure if you ever registered in our system (ZSSW) before? Check here.

For help? FAQ, Support Note

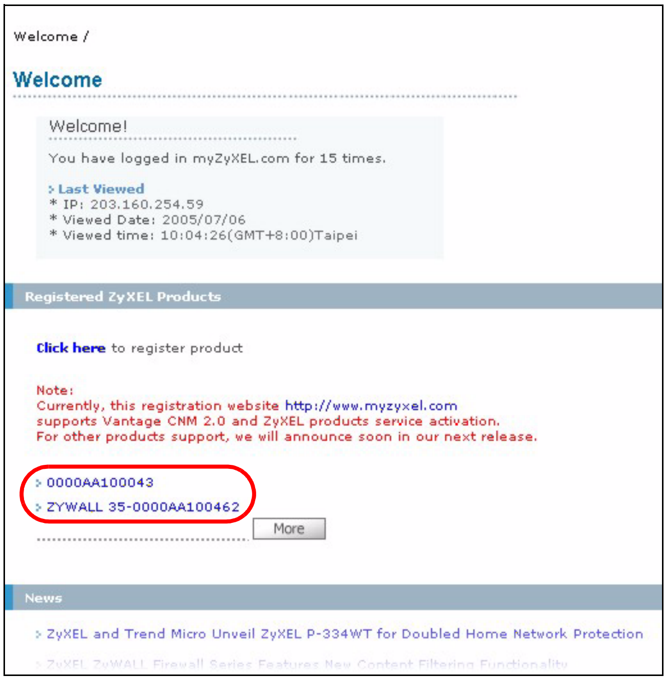
New User

> If you are not a registered user, Click here

3 A welcome screen displays. Click your ZyWALL's model name and/or MAC address under **Registered ZyXEL Products**. You can change the descriptive name for your

ZyWALL using the **Rename** button in the **Service Management** screen (see Figure 356 on page 484).

Figure 355 myZyXEL.com: Welcome



Welcome /

Welcome

Welcome!

You have logged in myZyXEL.com for 15 times.

Last Viewed
* IP: 203.160.254.59
* Viewed Date: 2005/07/06
* Viewed time: 10:04:26(GMT+8:00)Taipei

Registered ZyXEL Products

Click here to register product

Note:
Currently, this registration website http://www.myzyxel.com supports Vantage CNM 2.0 and ZyXEL products service activation.
For other products support, we will announce soon in our next release.

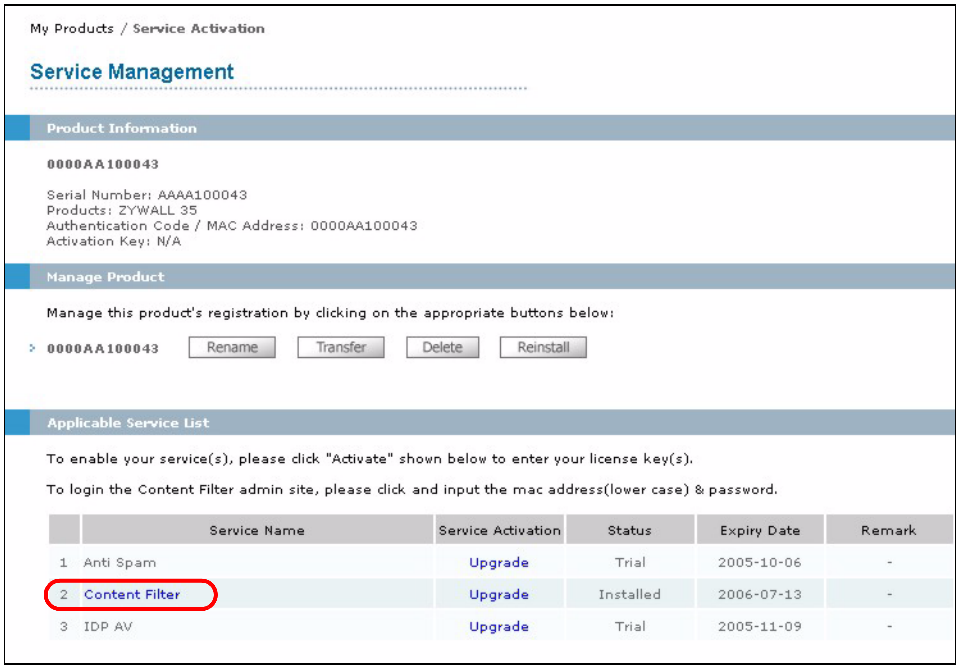
- 0000AA100043
- ZYWALL 35-0000AA100462

News

- ZyXEL and Trend Micro Unveil ZyXEL P-334WT for Doubled Home Network Protection
- ZyXEL ZyWALL Firewall Series Features New Content Filtering Functionality

4 In the **Service Management** screen click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.

Figure 356 myZyXEL.com: Service Management



My Products / Service Activation

Service Management

Product Information

0000AA100043

Serial Number: AAAA100043
Products: ZYWALL 35
Authentication Code / MAC Address: 0000AA100043
Activation Key: N/A

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

0000AA100043

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

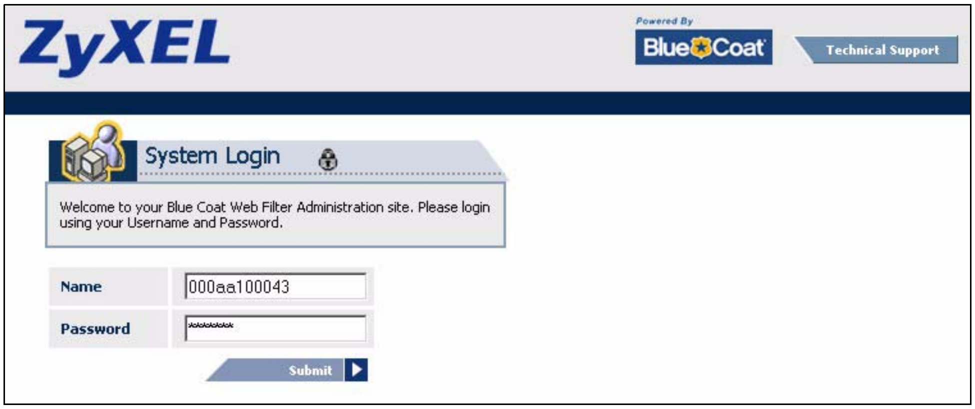
To login the Content Filter admin site, please click and input the mac address(lower case) & password.

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Anti Spam	Upgrade	Trial	2005-10-06	-
2	Content Filter	Upgrade	Installed	2006-07-13	-
3	IDP AV	Upgrade	Trial	2005-11-09	-

5 Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen (Figure 356 on page 484). Type your myZyXEL.com account password in the **Password** field.

6 Click **Submit**.

Figure 357 Blue Coat: Login


ZyXEL
Powered By
BlueCoat
Technical Support
Submit

System Login

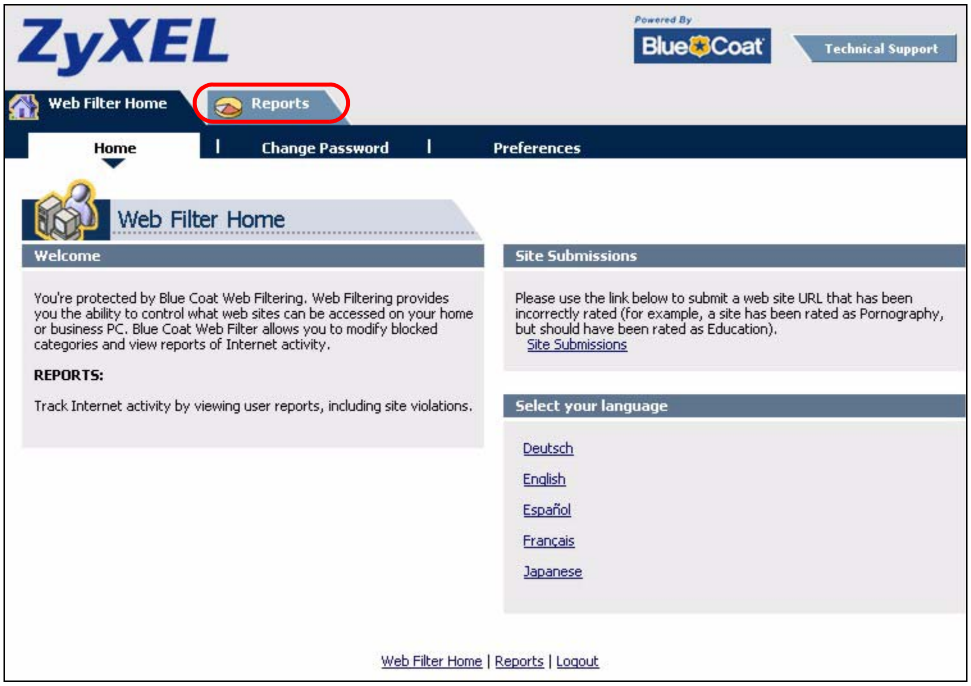
Welcome to your Blue Coat Web Filter Administration site. Please login using your Username and Password.

Name: 000aa100043

Password: ********

7 In the **Web Filter Home** screen, click the **Reports** tab.

Figure 358 Blue Coat Content Filter Reports Main Screen


ZyXEL
Powered By
BlueCoat
Technical Support
Web Filter Home
Reports
Home
Change Password
Preferences
Deutsch
English
Español
Français
Japanese
Web Filter Home | Reports | Logout

Web Filter Home

Welcome

You're protected by Blue Coat Web Filtering. Web Filtering provides you the ability to control what web sites can be accessed on your home or business PC. Blue Coat Web Filter allows you to modify blocked categories and view reports of Internet activity.

REPORTS:

Track Internet activity by viewing user reports, including site violations.

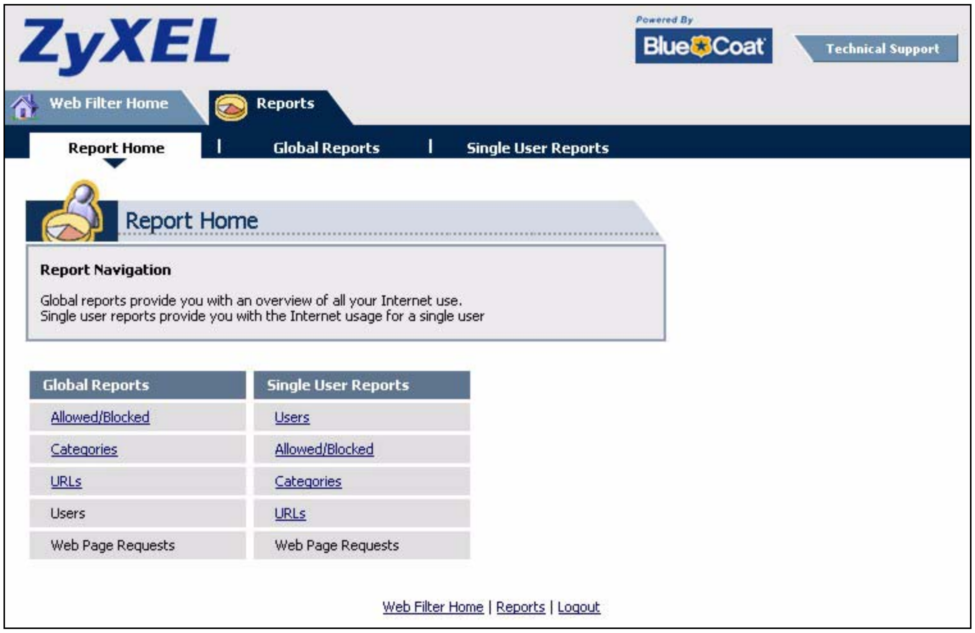
Site Submissions

Please use the link below to submit a web site URL that has been incorrectly rated (for example, a site has been rated as Pornography, but should have been rated as Education).
Site Submissions

Select your language

8 Select items under **Global Reports** or **Single User Reports** to view the corresponding reports.

Figure 359 Blue Coat: Report Home



ZyXEL
Powered By
Blue Coat
Technical Support
Web Filter Home
Reports
Report Home
Global Reports
Single User Reports
Report Home

Report Navigation

Global reports provide you with an overview of all your Internet use.
Single user reports provide you with the Internet usage for a single user

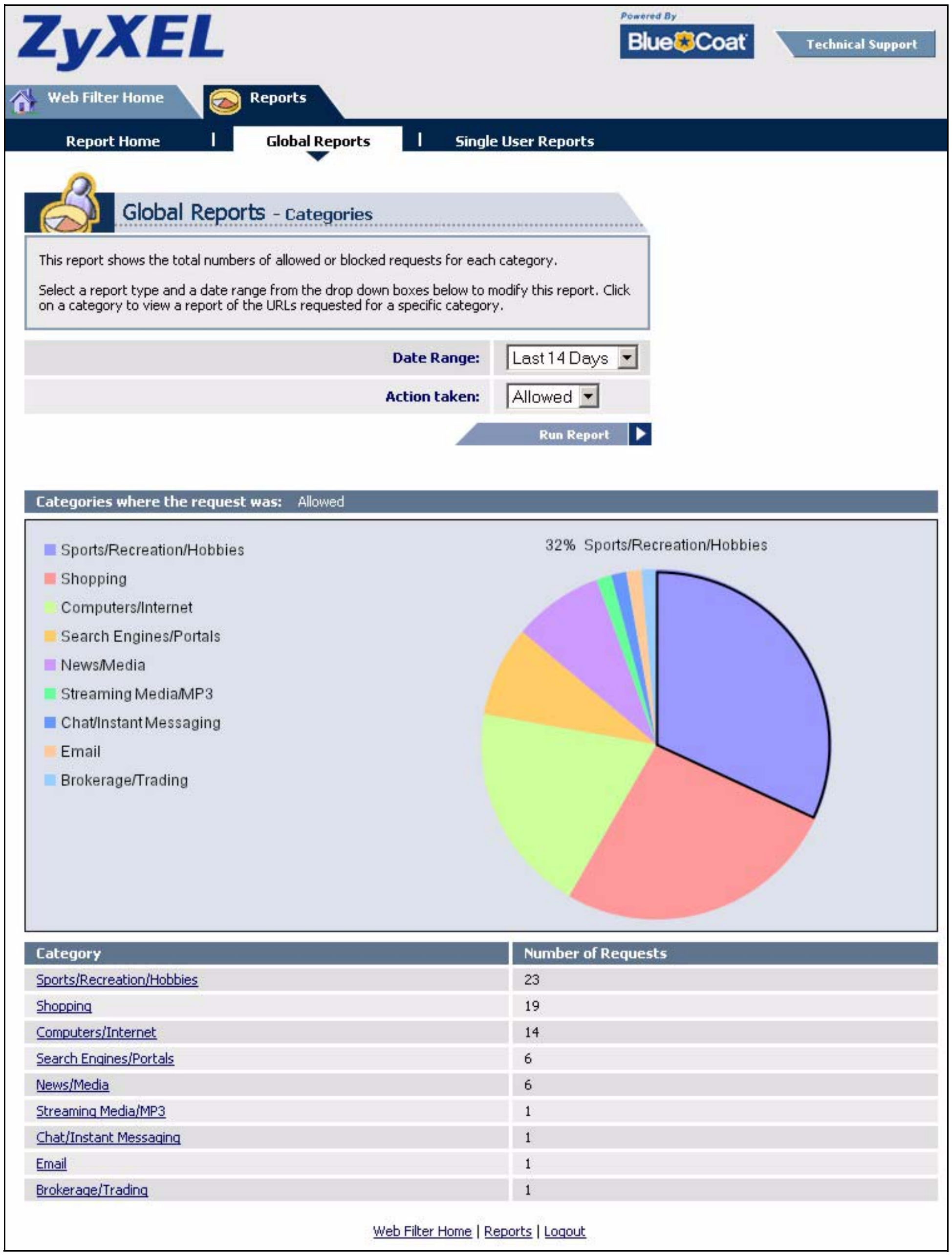
Global Reports	Single User Reports
Allowed/Blocked	Users
Categories	Allowed/Blocked
URLs	Categories
Users	URLs
Web Page Requests	Web Page Requests

Web Filter Home | Reports | Logout

9 Select a time period in the **Date Range** field, either **Allowed** or **Blocked** in the **Action Taken** field and a category (or enter the user name if you want to view single user reports) and click **Run Report**.The screens vary according to the report type you selected in the **Report Home** screen.

10 A chart and/or list of requested web site categories display in the lower half of the screen.

Figure 360 Global Report Screen Example


ZyXEL
Powered By
BlueCoat
Technical Support
Web Filter Home
Reports
Report Home
Global Reports
Single User Reports
Run Report
Sports/Recreation/Hobbies
Shopping
Computers/Internet
Search Engines/Portals
News/Media
Streaming Media/MP3
Chat/Instant Messaging
Email
Brokerage/Trading
32% Sports/Recreation/Hobbies
Web Filter Home | Reports | Logout

Global Reports - Categories

This report shows the total numbers of allowed or blocked requests for each category.

Select a report type and a date range from the drop down boxes below to modify this report. Click on a category to view a report of the URLs requested for a specific category.

Date Range: Last 14 Days

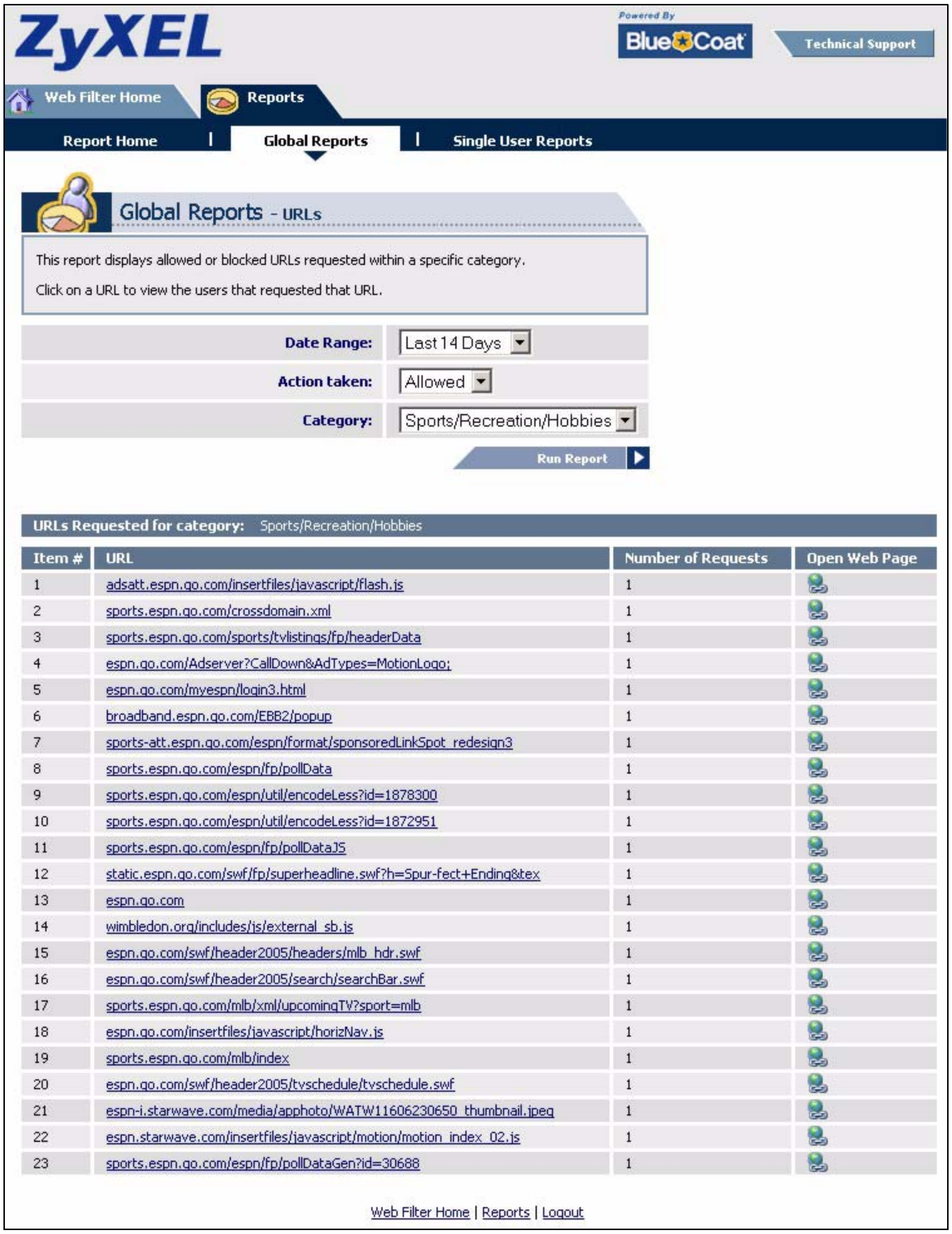
Action taken: Allowed

Categories where the request was: Allowed

Category	Number of Requests
Sports/Recreation/Hobbies	23
Shopping	19
Computers/Internet	14
Search Engines/Portals	6
News/Media	6
Streaming Media/MP3	1
Chat/Instant Messaging	1
Email	1
Brokerage/Trading	1

11 You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

Figure 361 Requested URLs Example



Global Reports - URLs

This report displays allowed or blocked URLs requested within a specific category.

Click on a URL to view the users that requested that URL.

Date Range: Last 14 Days

Action taken: Allowed

Category: Sports/Recreation/Hobbies

URLs Requested for category: Sports/Recreation/Hobbies

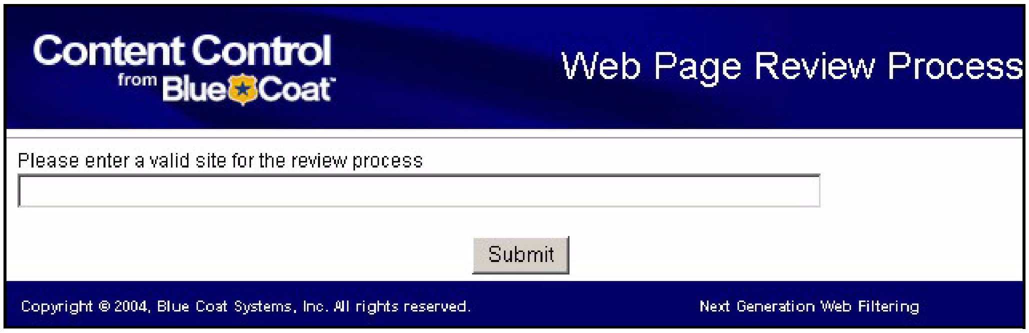
Item #	URL	Number of Requests	Open Web Page
1	adsatt.espn.go.com/insertfiles/javascript/flash.js	1	🌐
2	sports.espn.go.com/crossdomain.xml	1	🌐
3	sports.espn.go.com/sports/tvlistings/fp/headerData	1	🌐
4	espn.go.com/Adserver?CallDown&AdTypes=MotionLogo;	1	🌐
5	espn.go.com/myespn/login3.html	1	🌐
6	broadband.espn.go.com/EBB2/popup	1	🌐
7	sports-att.espn.go.com/espn/format/sponsoredLinkSpot_redesign3	1	🌐
8	sports.espn.go.com/espn/fp/pollData	1	🌐
9	sports.espn.go.com/espn/util/encodeLess?id=1878300	1	🌐
10	sports.espn.go.com/espn/util/encodeLess?id=1872951	1	🌐
11	sports.espn.go.com/espn/fp/pollDataJS	1	🌐
12	static.espn.go.com/swf/fp/superheadline.swf?h=Spur-fect+Ending&tex	1	🌐
13	espn.go.com	1	🌐
14	wimbledon.org/includes/js/external_sb.js	1	🌐
15	espn.go.com/swf/header2005/headers/mlb_hdr.swf	1	🌐
16	espn.go.com/swf/header2005/search/searchBar.swf	1	🌐
17	sports.espn.go.com/mlb/xml/upcomingTV?sport=mlb	1	🌐
18	espn.go.com/insertfiles/javascript/horizNav.js	1	🌐
19	sports.espn.go.com/mlb/index	1	🌐
20	espn.go.com/swf/header2005/tvschedule/tvschedule.swf	1	🌐
21	espn-i.starwave.com/media/apphoto/WATW11606230650_thumbnail.jpeg	1	🌐
22	espn.starwave.com/insertfiles/javascript/motion/motion_index_02.js	1	🌐
23	sports.espn.go.com/espn/fp/pollDataGen?id=30688	1	🌐

32.2 Web Site Submission

You may find that a web site has not been accurately categorized or that a web site's contents have changed and the content filtering category needs to be updated. Use the following procedure to submit the web site for review.

1. Log into the content filtering reports web site (see Section 32.1 on page 483).
2. In the **Web Filter Home** screen (see Figure 358 on page 485), click **Site Submissions** to open the **Web Page Review Process** screen shown next.

Figure 362 Web Page Review Process Screen


Content Control
from Blue Coat
Web Page Review Process

Please enter a valid site for the review process

Submit

Copyright © 2004, Blue Coat Systems, Inc. All rights reserved.

Next Generation Web Filtering

3 Type the web site's URL in the field and click **Submit** to have the web site reviewed.

PART V

Device HA & Objects

Device HA (493)
User/Group (503)
Addresses (515)
Services (521)
Schedules (527)
AAA Server (531)
Authentication Objects (541)
Certificates (545)
ISP Accounts (563)
SSL Application (567)

33

Device HA

Use device HA and Virtual Router Redundancy Protocol (VRRP) to increase network reliability. See Section 5.4.8 on page 117 for related information on these screens.

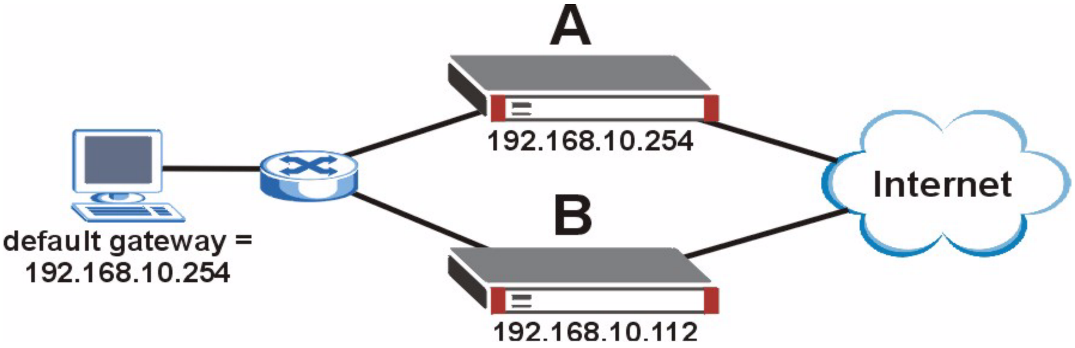
33.1 Virtual Router Redundancy Protocol (VRRP) Overview

Every computer on a network may send packets to a default gateway, which can become a single point of failure. Virtual Router Redundancy Protocol (VRRP) allows you to create redundant backup gateways to ensure that the default gateway is always available.

The ZyWALL runs VRRP v2. You can only set up device HA with other ZyWALLs of the same model running the same firmware version.

In VRRP, a virtual router represents a number of routers associated with one IP address, the IP address of the default gateway. Each virtual router is identified by a unique 8-bit identification number called a Virtual Router ID (VR ID). In the example below, Router **A** and Router **B** are part of virtual router 10 with IP address 192.168.10.254.

Figure 363 Example: VRRP, Normal Operation

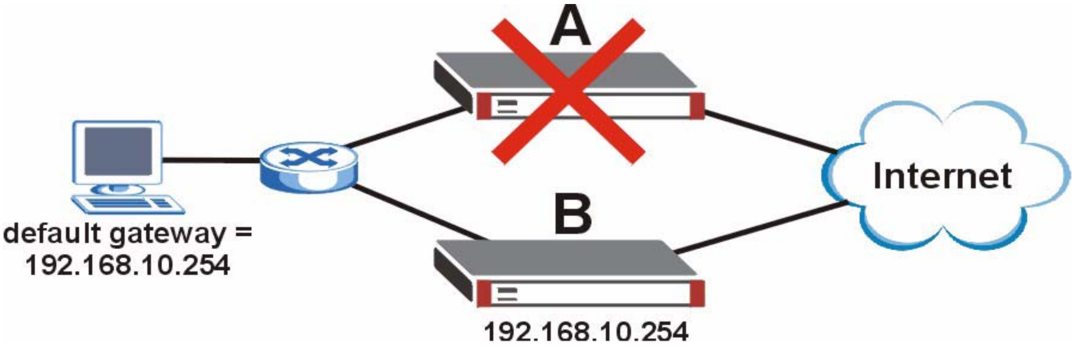


The VR ID is not shown. In normal operation, Router **A** is the master router. It has the same IP address as the default gateway and forwards traffic for the network. Router **B** is a backup router. It is using its management IP address 192.168.10.112. Router **A** sends regular messages to Router **B** to let Router **B** know that Router **A** is available. The time interval between these messages is called the advertisement interval.

Every router in a virtual router must use the same advertisement interval.

If Router **A** becomes unavailable, it stops sending messages to Router **B**. Router **B** detects this and assumes the role of the master router. This is illustrated below.

Figure 364 Example: VRRP, Master Becomes Unavailable



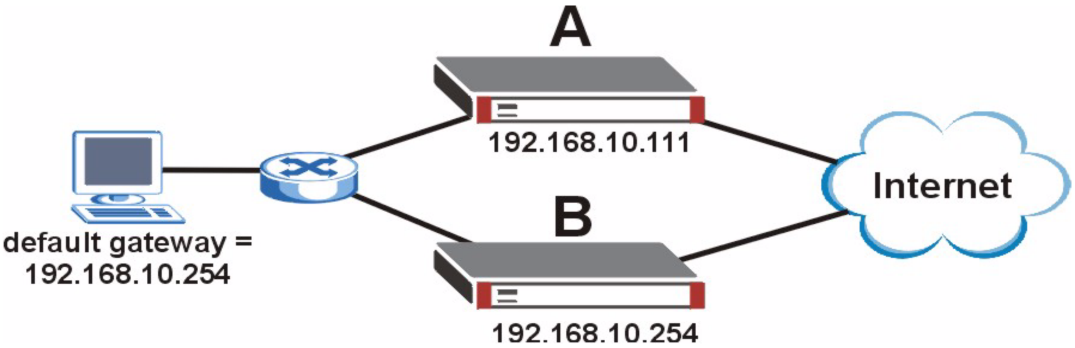
Router **B** is now using the IP address of the default gateway, and it is forwarding packets for the network. The loss of Router **A** has no effect on the network.

If there is more than one backup router, the backup router with the highest priority becomes the master router. The other backup routers remain backup routers.

If Router **A** becomes available again, one of two things can happen, depending on the settings in Router **A**.

1 Router **A** may preempt Router **B** and become the master router again. In this case, the network returns to the state shown in Figure 363 on page 493.
2 Router **A** returns to the network, but Router **B** remains the master router. This is illustrated below.

Figure 365 Example: VRRP, No Preempt



In this case, Router **A** becomes a backup router, and it uses its Manage IP, 192.168.10.111. Router **B** remains the master router until it becomes unavailable.

33.1.1 Additional VRRP Notes

- It is possible to set up two virtual routers so that they back up each other.
- VRRP uses IP protocol 112.

33.2 VRRP Group Overview

In the ZyWALL, you should create a VRRP group to add one of its interfaces to a virtual router. You can add any Ethernet or VLAN interface with a static IP address. You do not configure VRRP groups for virtual interfaces.

You can only use interfaces that have static IP addresses.

You can only enable one VRRP group for each interface, and you can only have one active VRRP group for each virtual router.

If you create a VRRP group for an Ethernet interface that has a VLAN interface configured on it, make sure you create a separate VRRP group for the VLAN interface. This will avoid an IP conflict if the backup ZyWALL takes over for the master.

You must set up a static IP address for the interface first, and this IP address should be the IP address of the virtual router, not the management IP address. The management IP address is assigned in the VRRP group. When the ZyWALL is the master router, the interface uses its IP address, the IP address of the virtual router. If the ZyWALL is a backup router, the interface uses its management IP address. You can look at the current IP address of the interface in the **Status** screen.

You can only have one active VRRP group for each interface, and you can only have one active VRRP group for each virtual router (VR ID).

If there is a PPPoE/PPTP interface on top of an interface in a VRRP group, the PPPoE/PPTP interface cannot connect to the ISP until the interface becomes the master in the virtual router.

At the time of writing, the advertisement interval is fixed at one second.

You can also set up authentication for a VRRP group. If you select AH MD5 authentication, the VRRP group uses IP protocol 51 (AH), instead of IP protocol 112 (VRRP).

33.2.1 Link Monitoring and Remote Management

With link monitoring enabled, a backup ZyWALL that takes over for an unavailable master ZyWALL takes over all of the master ZyWALL's static IP addresses. This way the backup ZyWALL takes over all of the master ZyWALL's functions. However, this also means you can no longer access the original master ZyWALL through one of its static IP addresses (because the backup ZyWALL now uses this address). Do one of the following to still be able to access the original master ZyWALL (assuming it is still functioning).

- Use a DHCP client interface. The DHCP server assigns the backup ZyWALL an IP address that is different from the IP address assigned to the master ZyWALL. So you can still access the original master ZyWALL through its DHCP assigned IP address. You will need some way to know the dynamic IP address assigned to the master ZyWALL's interface. One way is to set the master ZyWALL to use DDNS. Or, if you have access to the DHCP server, you can check it to see what IP address it assigned to the master ZyWALL.
- Use a static IP address on one of the master ZyWALL's interfaces without adding that interface to any VRRP group. Also leave the corresponding port on the backup ZyWALL unconnected. This way the original master ZyWALL still uses the static IP address after the backup ZyWALL takes over for it.
- Connect an external serial modem to the **AUX**port and configure dial-in management.

33.3 Device HA Screens

The **VRRP Group** summary screen provides information about which interfaces are in virtual routers and the role and status of each interface in the virtual router.

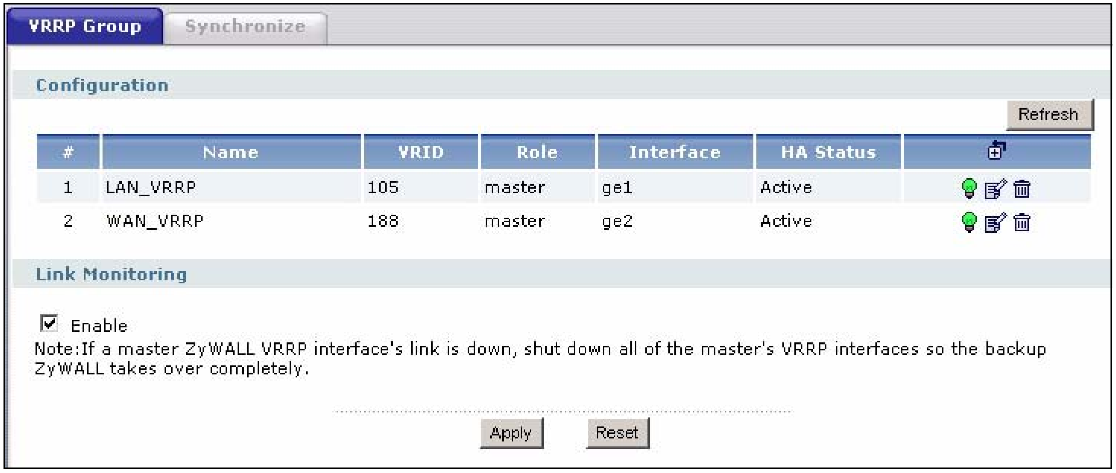
The **VRRP Group Add/Edit** screen allows you to add VRRP groups to the ZyWALL or to edit the configuration of an existing VRRP group. You have to go to the **VRRP Group** summary screen first to access this screen.

You can use the **Synchronize** screen to make sure all ZyWALLs in the VRRP group have the same updated certificates, AV signatures, IDP and application patrol signatures, system protect signatures, and configuration information, regardless of whether each router is the master router or a backup router.

33.4 VRRP Group Summary

The **VRRP Group** summary screen provides information about which interfaces are in virtual routers and the role and status of each interface in the virtual router. To access this screen, click **Device HA**.

Figure 366 Device HA > VRRP Group



#	Name	VRID	Role	Interface	HA Status	
1	LAN_VRRP	105	master	ge1	Active	
2	WAN_VRRP	188	master	ge2	Active	

☑ Enable

Note:If a master ZyWALL VRRP interface's link is down, shut down all of the master's VRRP interfaces so the backup ZyWALL takes over completely.

The following table describes the labels in this screen. See Section 33.5 on page 498 for more information as well.

Table 152 Device HA > VRRP Group

LABEL	DESCRIPTION
Refresh	Click this button to update the information in this screen.
#	This field is a sequential value, and it is not associated with a specific VRRP group.
Name	This field displays the name of the VRRP group.
VRID	This field displays the virtual router ID number.
Role	This field displays which role the interface plays in the virtual router. **Master** - This interface is the master interface in the virtual router. The interface always uses its static IP address, not the management IP address of the VRRP group. **Backup** - This interface is a backup interface in the virtual router. The interface may use its static IP address or the management IP address of the VRRP group, depending on whether or not the backup has become the master.
Interface	This field displays which interface is part of the virtual router.
HA Status	This field displays the status of the interface in the virtual router. **Active** - This interface is the master interface in the virtual router. **Stand-By** - This interface is a backup interface in the virtual router. **Fault** - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down. **n/a** - This interface is not connected to the virtual router. For example, this might happen when the VRRP group is first set up.
Add icon	This column provides icons to activate, deactivate, add, edit, and remove VRRP groups. To activate or deactivate a VRRP group, click the **Active** icon next to the group. Make sure you click **Apply** to save and apply the change. To add a VRRP group, click the **Add** icon at the top of the column. The **VRRP Group Add/Edit** screen appears. To edit a VRRP group, click the **Edit** icon next to the group. The **VRRP Group Add/Edit** screen appears. To delete a VRRP group, click the **Remove** icon next to the group. The web configurator confirms that you want to delete the VRRP group before doing so.
Link Monitoring	Enable link monitoring to have the master ZyWALL shut down all of its VRRP interfaces if one of its VRRP interface links goes down. This way the backup ZyWALL takes over all of the master ZyWALL’s functions.

Table 152 Device HA > VRRP Group (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

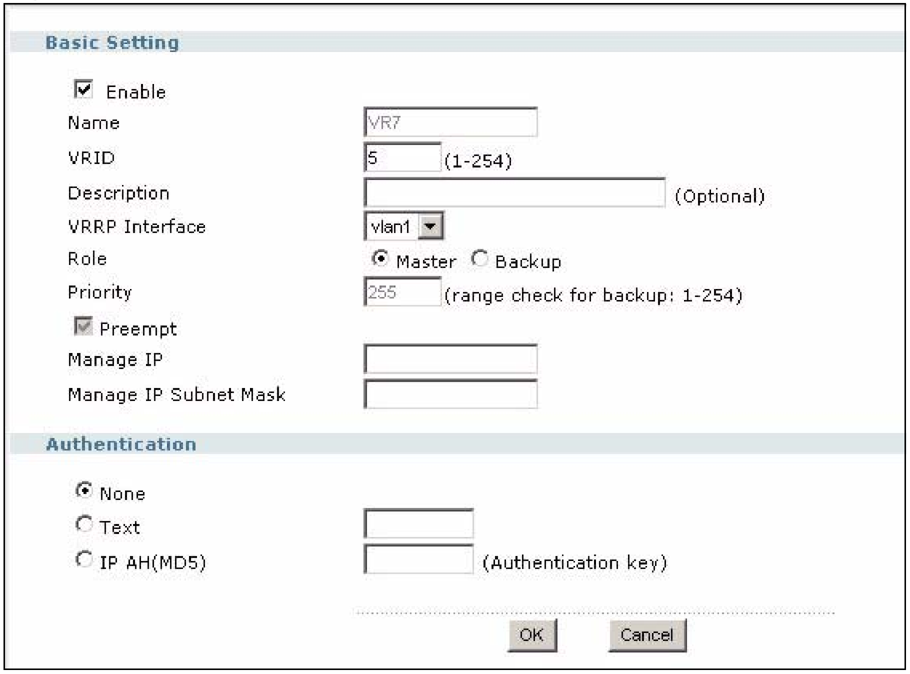
33.5 VRRP Group Add/Edit

The **VRRP Group Add/Edit** screen allows you to add VRRP groups to the ZyWALL or to edit the configuration of an existing VRRP group.

- You can only use interfaces that have static IP addresses. In addition, you should set the static IP address to the IP address of the virtual router.
- You can only enable one VRRP group for each interface.
- You can only have one active VRRP group for each virtual router (VR ID).

To access this screen, go to the **VRRP Group** summary screen (see Section 33.4 on page 496), and click either the **Add** icon or an **Edit** icon.

Figure 367 Device HA > VRRP Group > Edit



Basic Setting

☑ Enable

Name: VR7

VRID: 5 (1-254)

Description: (Optional)

VRRP Interface: vlan1

Role: ● Master ○ Backup

Priority: 255 (range check for backup: 1-254)

☑ Preempt

Manage IP:

Manage IP Subnet Mask:

Authentication

● None

○ Text

○ IP AH(MD5) (Authentication key)

The following table describes the labels in this screen.

Table 153 Device HA > VRRP Group > Edit

LABEL	DESCRIPTION
Enable	Select this to make the specified interface part of the virtual router. Clear this to take the specified interface out of the virtual router.
Name	This field is read-only if you are editing the VRRP group. Type the name of the VRRP group. This field must be unique in the ZyWALL, but it is not used in the virtual router. The virtual router uses the **VRID**. The name can consist of alphanumeric characters, the underscore, and the dash and may be up to fifteen characters long.

Table 153 Device HA > VRRP Group > Edit (continued)

LABEL	DESCRIPTION
VRID	Type the virtual router ID number.
Description	Type the description of the VRRP group. This field is only for your reference. It may be up to sixty printable ASCII characters long.
VRRP Interface	Select the interface in this device that is part of the virtual router. You can only select interfaces that have static IP addresses.
Role	Select the role that you want the interface plays in the virtual router. Choices are: **Master** - This interface is the master interface in the virtual router. The interface always uses its static IP address, not the management IP address of the VRRP group. Note: Do not set this field to **Master** for two or more routers in the same virtual router (same VR ID). **Backup** - This interface is a backup interface in the virtual router. The interface may use its static IP address or the management IP address of the VRRP group, depending on its current role. The current role depends on the other routers in the virtual router.
Priority	This field is available if the selected interface is a **Backup** interface. Type the priority of the backup interface. The backup interface with the highest value takes over the role of the master interface if the master interface becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.)
Preempt	This field is available if the selected interface is a **Backup** interface. Select this if the selected interface should become the master interface if a lower-priority interface is the master when this one is enabled. (If the role is **Master**, the interface preempts by default.)
Manage IP	This field is available if the selected interface is a **Backup** interface. Enter the IP address of the interface while it is in **Stand-By** mode. It is recommended that this IP address be in the same subnet as the interface. If it is not in the same subnet, the backup router cannot synchronize with the master via this VRRP interface.
Manage IP Subnet Mask	This field is available if the selected interface is a **Backup** interface.
Authentication	Select the authentication method used in the virtual router. Every interface in a virtual router must use the same authentication method and password. Choices are: **None** - this virtual router does not use any authentication method. **Text** - this virtual router uses a plain text password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long. **IP AH (MD5)** - this virtual router uses an encrypted MD5 password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long. See Section 13.1.2 on page 236 for more information about authentication methods.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

33.6 Synchronization Overview

In a virtual router, backup routers do not automatically get configuration updates from the master router. In this case, the master ZyWALL can send these updates to backup ZyWALLs. This is called synchronization.

During synchronization, the master ZyWALL sends the following information to the backup ZyWALL.

- Startup configuration file (**startup-config.conf**)
- AV signatures
- IDP and application patrol signatures
- System protect signatures
- Certificates (**My Certificates**, and **Trusted Certificates**)

Synchronization does not change the VRRP groups or synchronization settings in the backup ZyWALL, however.

Synchronization affects the entire device configuration. You can only configure one set of settings for synchronization, regardless of how many VRRP groups you might configure. The ZyWALL uses Secure FTP (on a port number you can change) to synchronize, but it is still recommended that the backup ZyWALL synchronize with a master ZyWALL on a secure network.

Synchronization can be either done manually or scheduled regularly, and it is initiated by the backup ZyWALL. The following restrictions apply.

- The backup ZyWALL must have at least one active VRRP group.
- The backup ZyWALL cannot be the master in any active VRRP group. This refers to the actual role at the time of synchronization, not the **Role** setting in the VRRP group.

During synchronization, the backup ZyWALL checks to see if the incoming configuration is different from the existing configuration on the backup. If the incoming configuration is different, the backup ZyWALL applies the entire configuration. The incoming configuration is not applied if it is the same as the existing configuration on the backup.

The backup ZyWALL is not available while it applies the new configuration. This usually takes two or three minutes but can take longer depending on the configuration complexity.

33.6.1 Synchronization and Subscription Services

The backup ZyWALL must have its own (separate) licenses for services like IDP/AppPatrol, Anti-Virus, Content Filtering, and SSL VPN.

Backup ZyWALLs can only get updates for services to which they have subscribed. For example, if a backup ZyWALL is subscribed to IDP/AppPatrol, but not Anti-Virus, it gets IDP/AppPatrol updates from the master ZyWALL, but not Anti-Virus updates. It is highly recommended that you subscribe the backup ZyWALL to the same services as you subscribe the master ZyWALL.

You must subscribe to services on the backup ZyWALL before synchronizing it with the master ZyWALL.

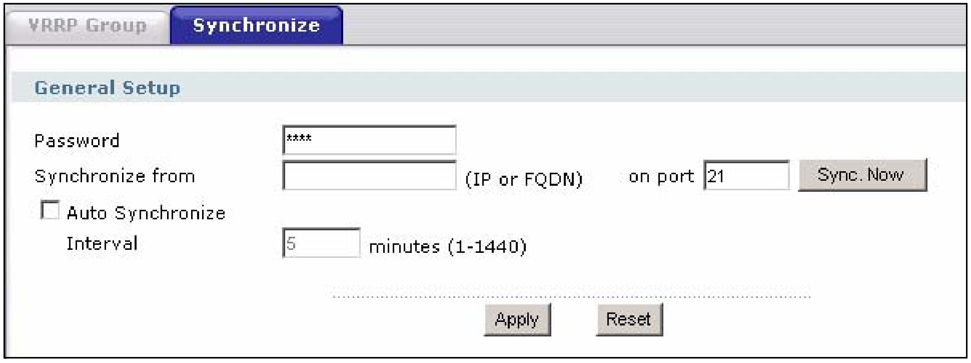
33.6.2 Synchronize Screen

Use this screen if you want the ZyWALL to get or to send updated IDP signatures, and configuration information in the virtual router.

You can only set up synchronization with other ZyWALLs of the same model running the same firmware version.

To access this screen, click **Network** > **Device HA** > **Synchronize**.

Figure 368 Network > Device HA > Synchronize



Password: ****

Synchronize from:

on port: 21

☐ Auto Synchronize

Interval: 5 minutes (1-1440)

For synchronization, every ZyWALL in a virtual router should usually have the same **Password**, **Synchronize From**, and **on port** values. In addition, the management IP address must be in the same subnet as the interface (in other words, the virtual router). The following table describes the labels in this screen.

Table 154 Network > Device HA > Synchronize

LABEL	DESCRIPTION
Password	Enter the password used to verify other ZyWALL routers during synchronization. This password is different than the one that is used for authentication in the VRRP group. Every ZyWALL in the virtual router must use the same password. If you leave this field blank, the password returns to its default setting “1234”.
Synchronize from	Enter the IP address or fully-qualified domain name (FQDN) of the router from which to get updated configuration and IDP signatures. Usually, you should enter the IP address or FQDN of a virtual router on a secure network.
on port	Enter the Secure FTP port number used by the ZyWALL you specified in **Synchronize from**. Usually, every ZyWALL in the virtual router should use the same port number. Otherwise, if the master ZyWALL changes, you might have to change this port number.

Table 154 Network > Device HA > Synchronize (continued)

LABEL	DESCRIPTION
Sync. Now	Click this button to get updated certificates, AV signatures, IDP and application patrol signatures, system protect signatures, and configuration information from the specified ZyWALL router. Note: If the new configuration is different from the existing one on this backup ZyWALL, this backup ZyWALL applies the entire configuration.
Auto Synchronize	Select this to get updated configuration and IDP signatures automatically from the specified ZyWALL according to the specified **Interval**. The first synchronization begins after the specified **Interval**; the ZyWALL does not synchronize immediately.
Interval	This field is only available if **Auto Synchronize** is checked. Type the number of minutes to wait between synchronizations. This value must be a number between 1 and 1440 (one day).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

34

User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the ZyWALL. You can also set up rules that control when users have to log in to the ZyWALL before the ZyWALL routes traffic for them. See Section 5.5.1 on page 122 for related information on these screens.

34.1 User Account Overview

A user account defines the privileges of a user logged into the ZyWALL. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the ZyWALL.

34.1.1 User Types

These are the types of user accounts the ZyWALL uses.

Table 155 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change ZyWALL configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at ZyWALL configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
Guest	Access network services	WWW
Ext-User	External User Account	WWW

The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 38 on page 531 for more information about authentication methods.)

34.1.2 Ext-User Accounts

Set up an **Ext-User** account if the user is authenticated by an external server and you want to set up specific policies for this user in the ZyWALL. If you do not want to set up policies for this user, you do not have to set up an **Ext-User** account.

Ext-User users should be authenticated by an external server, such as LDAP or RADIUS. If the ZyWALL tries to use the local database to authenticate an **Ext-User**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in Chapter 38 on page 531 and Chapter 39 on page 541, respectively.)

If the ZyWALL tries to authenticate an **Ext-User** using the local database, the attempt always fails.

Once an **Ext-User** user has been authenticated, the ZyWALL tries to get the user type (see Table 155 on page 503) from the external server. If the external server does not have the information, the ZyWALL sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the ZyWALL checks the following places, in order.

1. User account in the remote server.
2. User account (Ext-User) in the ZyWALL.
3. Default user account for LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the ZyWALL.

See Section 34.1.2.1 on page 504 for a list of attributes and how to set up the attributes in an external server.

34.1.2.1 Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 156 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	**User Type**. Possible Values: admin, limited-admin, user, guest.
leaseTime	**Lease Time**. Possible Values: 1-1440 (minutes).
reauthTime	**Reauthentication Time**. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 369 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 370 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

34.1.2.2 Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the web configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts. See Chapter 45 on page 615 for more information about shell scripts.

34.1.3 User Groups

Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one. User groups may consist of user accounts or other user groups, but you cannot put access users and admin users in the same user group.

You cannot put access users and admin users in the same user group.

In addition, you cannot put the default **admin** account into any user group.

You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

34.1.4 Access Users and the ZyWALL

By default, access users do not have to log in to the ZyWALL to use the network services it provides. The ZyWALL automatically routes packets for everyone. In this case, the ZyWALL does not enforce any user-aware policies, but you can still set up policies based on IP address or other criteria.

If you want to enforce user-aware policies, access users must log in to the ZyWALL first. In this case, they should go to the appropriate IP address (or domain name, if you set up DNS) to log in to the ZyWALL. (See Section 34.5 on page 513.) You can provide an incentive to do this by preventing access users from using network services until they log in.

34.1.5 Force User Authentication Policy

Instead of making users to go to the **Login** screen manually, you can configure the ZyWALL to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet. Then, the ZyWALL can enforce user-aware policies.

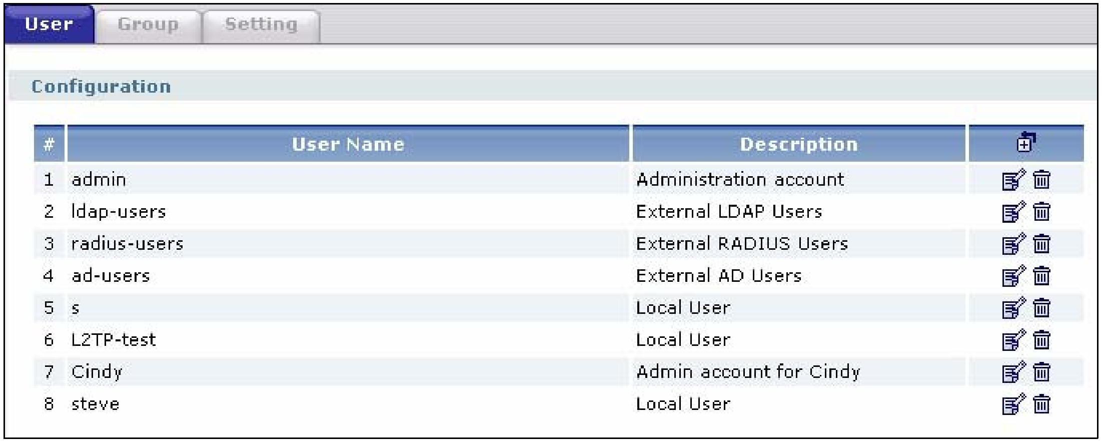
This works with HTTP traffic only. The ZyWALL does not force users to log in before it routes other kinds of traffic.

The ZyWALL does not automatically route the request that prompted the login, however, so users have to make this request again.

34.2 User Summary

The **User** screen provides a summary of all user accounts. To access this screen, login to the web configurator, and click **User/Group**.

Figure 371 User/Group



#	User Name	Description
1	admin	Administration account
2	ldap-users	External LDAP Users
3	radius-users	External RADIUS Users
4	ad-users	External AD Users
5	s	Local User
6	L2TP-test	Local User
7	Cindy	Admin account for Cindy
8	steve	Local User

The following table describes the labels in this screen.

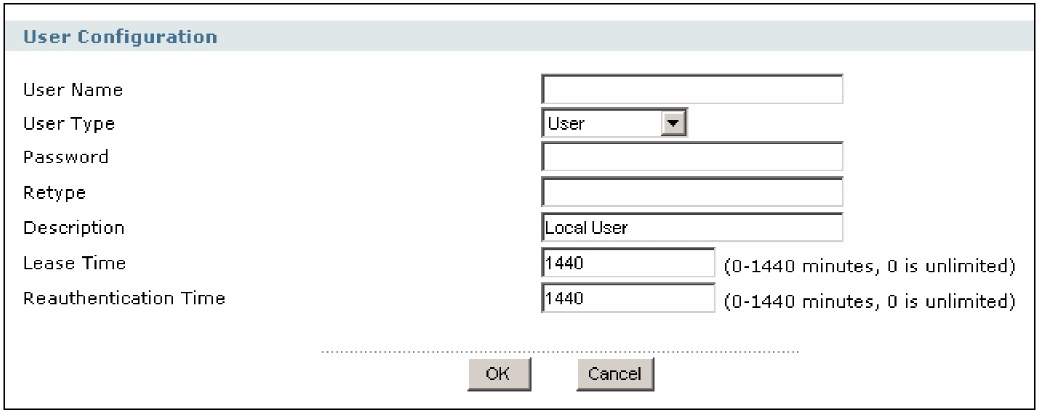
Table 157 User/Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
Description	This field displays the description for each user.
Add icon	This column provides icons to add, edit, and remove users. To add a user, click the **Add** icon at the top of the column. The **User Add/Edit** screen appears. To edit a user, click the **Edit** icon next to the user. The **User Add/Edit** screen appears. To delete a user, click the **Remove** icon next to the user. The web configurator confirms that you want to delete the user before doing so.

34.2.1 User Add/Edit

The **User Add/Edit** screen allows you to create a new user account or edit an existing one. To access this screen, go to the **User** screen (see Section 34.2 on page 506), and click either the **Add** icon or an **Edit** icon.

Figure 372 User/Group > User > Edit



User Name	
User Type	User
Password	
Retype	
Description	Local User
Lease Time	1440 (0-1440 minutes, 0 is unlimited)
Reauthentication Time	1440 (0-1440 minutes, 0 is unlimited)

The following table describes the labels in this screen.

Table 158 User/Group > User > Edit

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 34.2.1.1 on page 508.
User Type	Select what type of user this is. Choices are: • **Admin** - this user can look at and change the configuration of the ZyWALL • **Limited-Admin** - this user can look at the configuration of the ZyWALL but not to change it • **User** - this user has access to the ZyWALL's services but cannot look at the configuration • **Guest** - this user has access to the ZyWALL's services but cannot look at the configuration • **Ext-User** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Section 34.1.2 on page 504 for more information about this type.
Password	This field is not available if you select the **Ext-User** user type. Enter the password of this user account. It can consist of 4 - 30 alphanumeric characters.
Retype	This field is not available if you select the **Ext-User** user type. Enter the password again.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Lease Time	Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the web configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 34.4 on page 510), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this user can be logged into the ZyWALL in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

34.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not ‘bob’.
- User names have to be different than user group names.
- Reserved user names are listed in the following table.

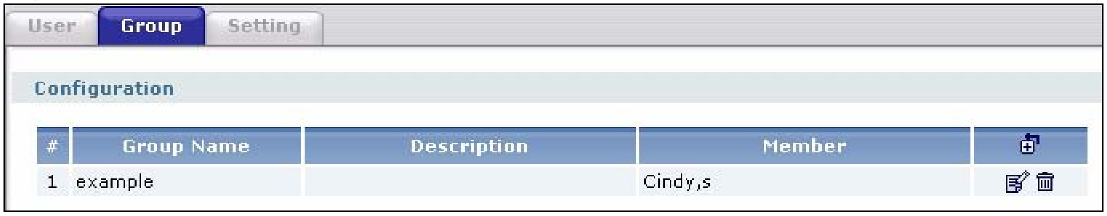
Table 159 Reserved User Names

- adm
- admin
- any
- bin
- daemon
- debug
- devicehaecived
- ftp
- games
- halt
- ldap-users
- lp
- mail
- news
- nobody
- operator
- radius-users
- root
- shutdown
- sshd
- sync
- uucp
- zyxel

34.3 Group Summary

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the web configurator, and click **User/Group** > **Group**.

Figure 373 User/Group > Group



#	Group Name	Description	Member
1	example		Cindy,s

The following table describes the labels in this screen. See Section 34.3.1 on page 509 for more information as well.

Table 160 User/Group > Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.

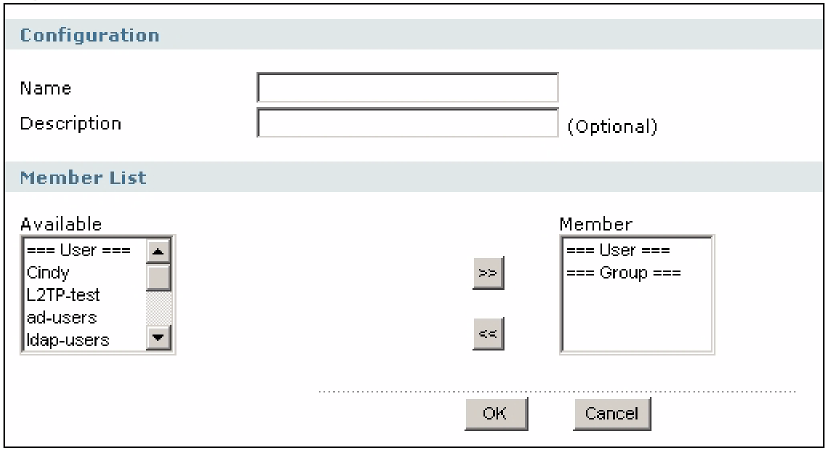
Table 160 User/Group > Group (continued)

LABEL	DESCRIPTION
Member	This field lists the members in the user group. Each member is separated by a comma.
Add icon	This column provides icons to add, edit, and remove user groups. To add a user group, click the **Add** icon at the top of the column. The **Group Add/Edit** screen appears. To edit a user group, click the **Edit** icon next to the user group. The **Group Add/Edit** screen appears. To delete a user group, click the **Remove** icon next to the user group. The web configurator confirms that you want to delete the user group before doing so. If you delete the group, you do not delete the users in the group.

34.3.1 Group Add/Edit

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see Section 34.3 on page 508), and click either the **Add** icon or an **Edit** icon.

Figure 374 User/Group > Group > Add



The following table describes the labels in this screen.

Table 161 User/Group > Group > Add

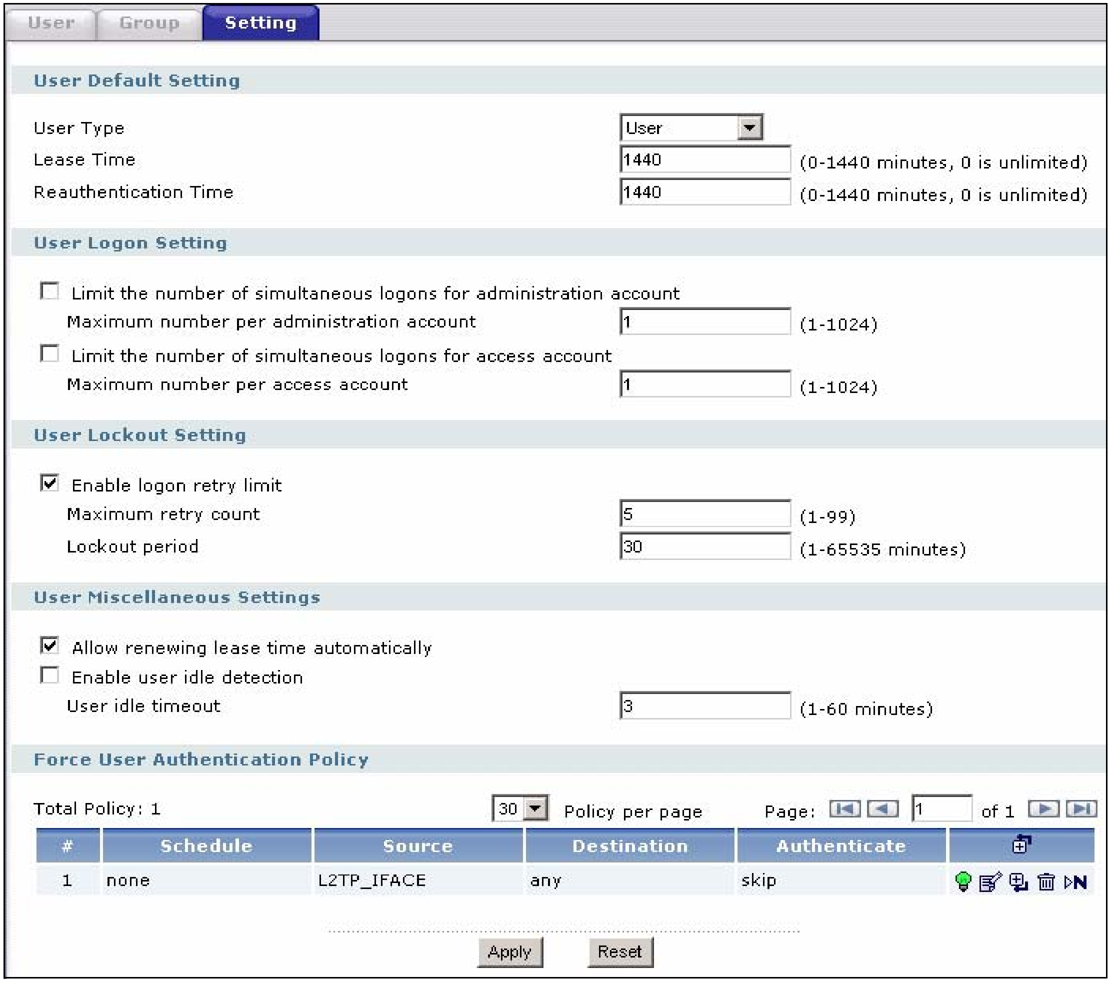
LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Available	This field displays the names of the users and user groups that can be added to the user group. Select users and groups that you want to be members of this group and click the right arrow to add them to the member list.
Member	This field displays the names of the users and user groups that have been added to the user group. The order of members is not important. To remove members, select them and click the left arrow.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

34.4 Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the ZyWALL. You can also use this screen to specify when users must log in to the ZyWALL before it routes traffic for them.

To access this screen, login to the web configurator, and click **User/Group** > **Setting**.

Figure 375 User/Group > Setting



User Default Setting

User Type: User

Lease Time: 1440 (0-1440 minutes, 0 is unlimited)

Reauthentication Time: 1440 (0-1440 minutes, 0 is unlimited)

User Logon Setting

☐ Limit the number of simultaneous logons for administration account

Maximum number per administration account: 1 (1-1024)

☐ Limit the number of simultaneous logons for access account

Maximum number per access account: 1 (1-1024)

User Lockout Setting

☑ Enable logon retry limit

Maximum retry count: 5 (1-99)

Lockout period: 30 (1-65535 minutes)

User Miscellaneous Settings

☑ Allow renewing lease time automatically

☐ Enable user idle detection

User idle timeout: 3 (1-60 minutes)

Force User Authentication Policy

Total Policy: 1   30 Policy per page   Page: 1 of 1

#	Schedule	Source	Destination	Authenticate	
1	none	L2TP_IFACE	any	skip	

The following table describes the labels in this screen.

Table 162 User/Group > Setting

LABEL	DESCRIPTION
User Default Setting	
User Type	Select the default user type when you create a new user account. You can still change the user type for each user account.
Lease Time	Select the default lease time when you create a new user account. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. You can still change the lease time for each user account.
Reauthentication Time	Select the default reauthentication time when you create a new user account. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. You can still change the reauthentication time for each user account.

Table 162 User/Group > Setting (continued)

LABEL	DESCRIPTION
User Logon Setting	
Limit ... for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user. The number must be between 1 and 1024.
Limit ... for access account	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.
Maximum number per access account	This field is effective when **Limit ... for access account** is checked. Type the maximum number of simultaneous logins by each access user. The number must be between 1 and 1024.
User Lockout Setting	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
User Miscellaneous Setting	
Allow renewing lease time ...	Select this check box if access users can renew lease time automatically, as well as manually, simply by checking the **Updating lease time automatically** check box on their screen.
Enable user idle detection	This is applicable for access users. Select this check box if you want the ZyWALL to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The ZyWALL automatically logs out the access user once the **User idle timeout** has been reached.
User idle timeout	This is applicable for access users. This field is effective when **Enable user idle detection** is checked. Type the number of minutes each access user can be logged in and idle before the ZyWALL automatically logs out the access user.
Force User Authentication Policy	Use this section to specify when users must log in to the ZyWALL before the ZyWALL routes HTTP traffic for them. Once users have logged in, the ZyWALL can enforce user-aware policies. This section displays the conditions that are applied, in sequence, to decide what the appropriate action is. By default, users do not have to log in to the ZyWALL.
Total Policy	This is the number of entries configured.
Policy per page	Select how many entries to display per page in the screen.

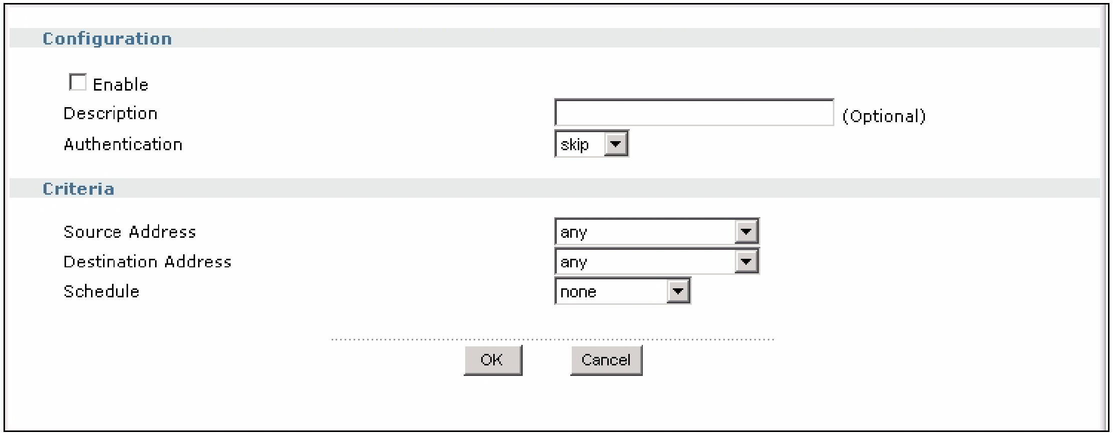
Table 162 User/Group > Setting (continued)

LABEL	DESCRIPTION
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific condition.
Schedule	This field displays the schedule object that specifies when this condition applies. It displays **none** if this condition always applies.
Source	This field displays the source address object of traffic to which this condition applies. It displays **any** if this condition applies to traffic from all source addresses.
Destination	This field displays the destination address object of traffic to which this condition applies. It displays **any** if this condition applies to traffic from all destination addresses.
Authenticate	This field displays whether users must log in (**force**) or whether users do not have to log in (**skip**) when this condition is checked and satisfied.
Add icon	This column provides icons to add, edit, move, and remove conditions. It also provides icons to activate and deactivate conditions. To add a condition, click the **Add** icon at the top of the column or next to each condition. If you click the one at the top of the column, the new condition is first in the list. If you click the one next to a condition, the new condition appears right below this condition. To edit a condition, click the **Edit** icon at the top of the column or next to each condition. The **Force User Authentication Policy Add/Edit** screen appears. To remove a condition, click on the **Remove** icon next to the condition. The web configurator confirms that you want to delete the condition before doing so. To move a condition up or down in the list, click on the **Move to N** icon next to the condition, and type the line number (**#** field) where you want to move this condition. The **#** field is updated accordingly. To activate or deactivate a condition, click the **Active** icon next to the condition. Make sure you click **Apply** to save and apply the change.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to start configuring this screen again.

34.4.1 Force User Authentication Policy Add/Edit

Use this screen to specify a condition when users must log in or do not have to log in to the ZyWALL before their HTTP traffic can pass through the ZyWALL.

Figure 376 User/Group > Setting > Force User Authentication Policy > Add/Edit



Configuration

☐ Enable

Description: (Optional)

Authentication: skip

Criteria

Source Address: any

Destination Address: any

Schedule: none

The following table describes the labels in this screen.

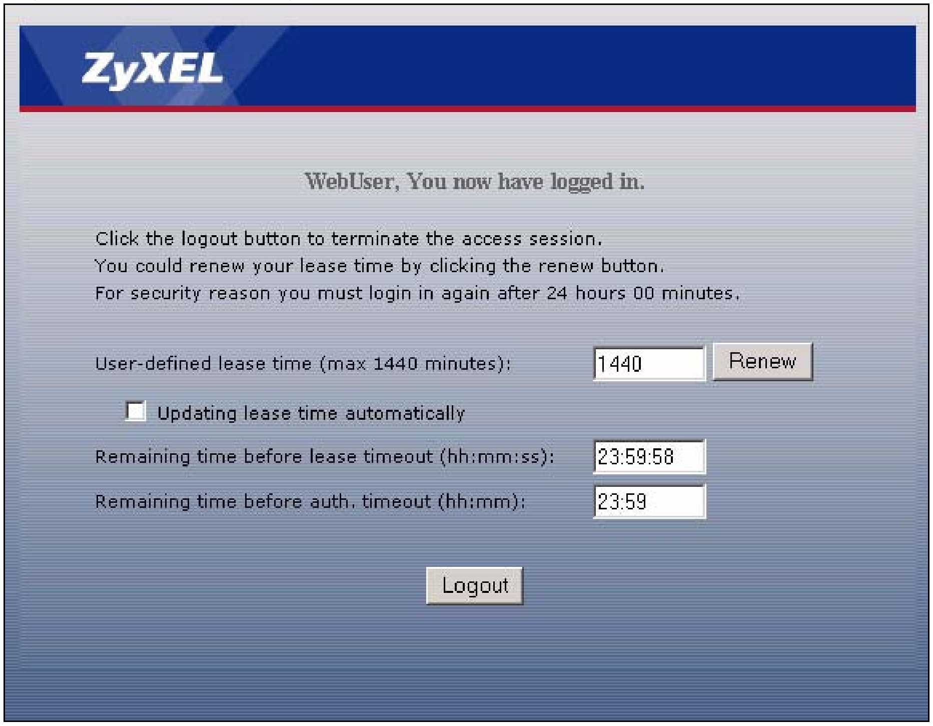
Table 163 User/Group > Setting > Force User Authentication Policy > Add/Edit

LABEL	DESCRIPTION
Enable	Select this if you want this condition to be active.
Description	Enter a description for this condition. It can be up to 60 printable ASCII characters long.
Authentication	Select whether users must log in (**force**) or whether users do not have to log in (**skip**) when this condition is checked and satisfied.
Source Address	Select a source IP address object or select **Create Object** to configure a new one. Select **any** if this condition applies to traffic from all source addresses.
Destination Address	Select the destination address of traffic to which this condition applies or select **Create Object** to configure a new one. Select **any** if this condition applies to traffic from all destination addresses.
Schedule	Select the schedule object that specifies when this condition applies or select **Create Object** to configure a new one (see Chapter 37 on page 527 for details). Select **none** if this condition always applies.
OK	Select this to save your changes and return to the previous screen.
Cancel	Select this to return to the previous screen without saving any changes.

34.5 Web Configurator for Non-Admin Users

Access users cannot use the Web configurator to browse the configuration of the ZyWALL. Instead, when access users log in to the ZyWALL (forced in the screen as shown in Figure 375 on page 510 or otherwise), the following screen appears.

Figure 377 Web Configurator for Non-Admin Users



WebUser, You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the renew button.
For security reason you must login in again after 24 hours 00 minutes.

User-defined lease time (max 1440 minutes): 1440

☐ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 23:59:58

Remaining time before auth. timeout (hh:mm): 23:59

The following table describes the labels in this screen.

Table 164 Web Configurator for Non-Admin Users

LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the ZyWALL automatically logs them out. The ZyWALL sets this amount of time according to the • **User-defined lease time** field in this screen • **Lease time** field in the **User Add/Edit** screen (see Section 34.2.1 on page 506) • **Lease time** field in the **Setting** screen (see Section 34.4 on page 510)
Updating lease time automatically	This box appears if you checked the **Allow renewing lease time automatically** box in the **Setting** screen. (See Section 34.4 on page 510.) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the **Renew** button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the ZyWALL automatically logs the access user out, regardless of the lease time.

35

Addresses

This chapter describes how to set up addresses and address groups for the ZyWALL. See Section 5.5 on page 122 for related information on these screens.

35.1 Addresses Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

35.2 Address Screens

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

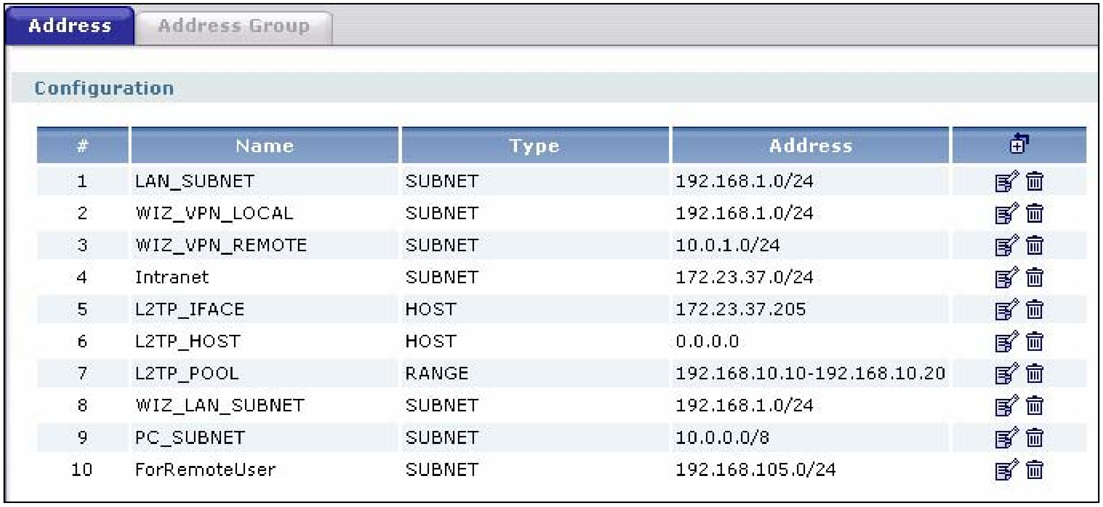
- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.
- **SUBNET** - a network address is defined by a **Network** IP address and **Netmask** subnet mask.

There are two different screens, the **Address** summary screen and the **Address Add/Edit** screen.

35.2.1 Address Summary

The **Address** screen provides a summary of all addresses in the ZyWALL. To access this screen, click **Object** > **Address > Address**.

Figure 378 Object > Address > Address



#	Name	Type	Address
1	LAN_SUBNET	SUBNET	192.168.1.0/24
2	WIZ_VPN_LOCAL	SUBNET	192.168.1.0/24
3	WIZ_VPN_REMOTE	SUBNET	10.0.1.0/24
4	Intranet	SUBNET	172.23.37.0/24
5	L2TP_IFACE	HOST	172.23.37.205
6	L2TP_HOST	HOST	0.0.0.0
7	L2TP_POOL	RANGE	192.168.10.10-192.168.10.20
8	WIZ_LAN_SUBNET	SUBNET	192.168.1.0/24
9	PC_SUBNET	SUBNET	10.0.0.0/8
10	ForRemoteUser	SUBNET	192.168.105.0/24

The following table describes the labels in this screen. See Section 35.2.2 on page 516 for more information as well.

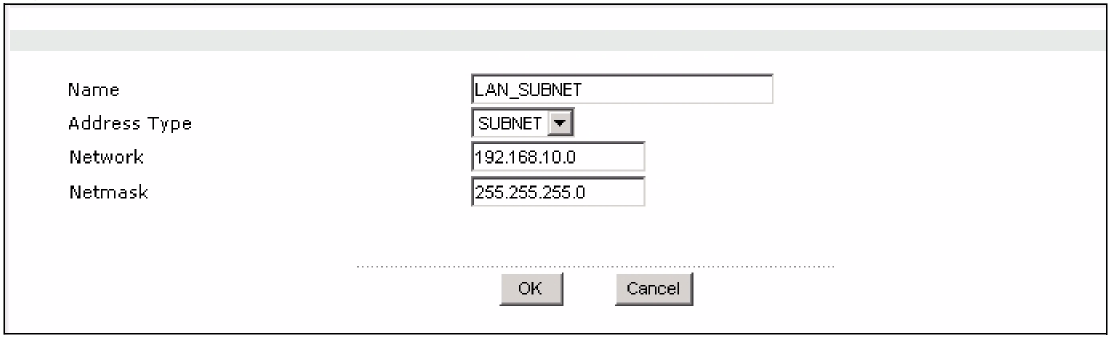
Table 165 Object > Address > Address

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the name of each address.
Type	This field displays the type of each address.
Address	This field displays the IP addresses represented by each address object.
Add icon	This column provides icons to add, edit, and remove addresses. To add an address, click the **Add** icon at the top of the column. The **Address Add/Edit** screen appears. To edit an address, click the **Edit** icon next to the address. The **Address Add/Edit** screen appears. To delete an address, click on the **Remove** icon next to the address. The web configurator confirms that you want to delete the address before doing so.

35.2.2 Address Add/Edit

The **Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 35.2.1 on page 515), and click either the **Add** icon or an **Edit** icon.

Figure 379 Object > Address > Address > Edit



Name LAN_SUBNET
Address Type SUBNET
Network 192.168.10.0
Netmask 255.255.255.0

The following table describes the labels in this screen.

Table 166 Object > Address > Address > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: **HOST**, **RANGE**, and **SUBNET**.
IP Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

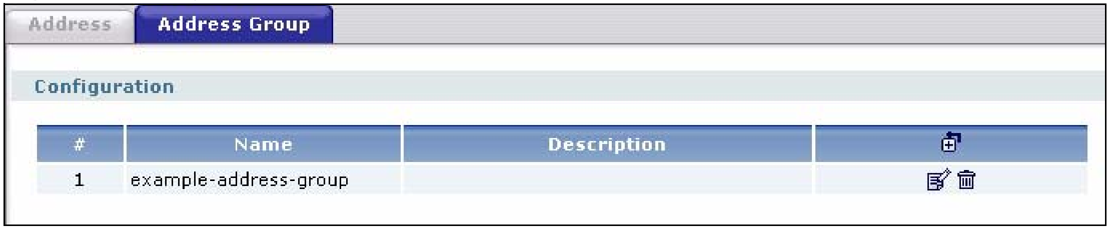
35.3 Address Group Screens

Use the **Address Group** summary screen and the **Address Group Add/Edit** screen, to maintain address groups in the ZyWALL.

35.3.1 Address Group Summary

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Object** > **Address** > **Address Group**.

Figure 380 Object > Address > Address Group



#	Name	Description	
1	example-address-group		

The following table describes the labels in this screen. See Section 35.3.2 on page 518 for more information as well.

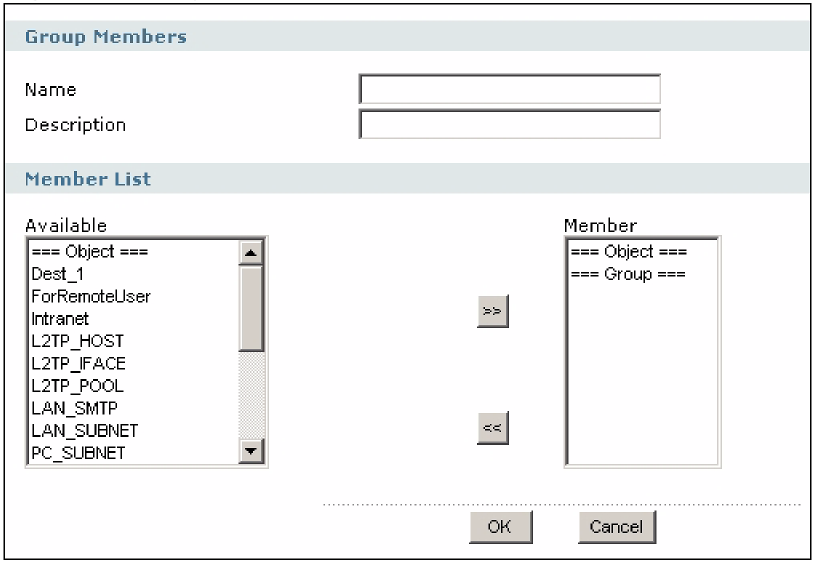
Table 167 Object > Address > Address Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Add icon	This column provides icons to add, edit, and remove address groups. To add an address group, click the **Add** icon at the top of the column. The **Address Group Add/Edit** screen appears. To edit an address group, click the **Edit** icon next to the address group. The **Address Group Add/Edit** screen appears. To delete an address group, click on the **Remove** icon next to the address group. The web configurator confirms that you want to delete the address group.

35.3.2 Address Group Add/Edit

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see Section 35.3.1 on page 517), and click either the **Add** icon or an **Edit** icon.

Figure 381 Object > Address > Address Group > Add


Group Members
Name
Description
Member List
Available
=== Object ===
Dest_1
ForRemoteUser
Intranet
L2TP_HOST
L2TP_IFACE
L2TP_POOL
LAN_SMTP
LAN_SUBNET
PC_SUBNET
>>
<<
Member
=== Object ===
=== Group ===
OK
Cancel

The following table describes the labels in this screen.

Table 168 Object > Address > Address Group > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.

Table 168 Object > Address > Address Group > Add (continued)

LABEL	DESCRIPTION
Available	This field displays the names of the address and address group objects that can be added to the address group. Select address and address group objects that you want to be members of this group and click the right arrow to add them to the member list.
Member	This field displays the names of the address and address group objects that have been added to the address group. The order of members is not important. To remove members, select them and click the left arrow.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

36

Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features. See Section 5.5 on page 122 for related information on these screens.

36.1 Services Overview

See Appendix C on page 703 for a list of commonly-used services.

36.1.1 IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

36.1.2 Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications

- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, firewall rules, and IDP profiles.

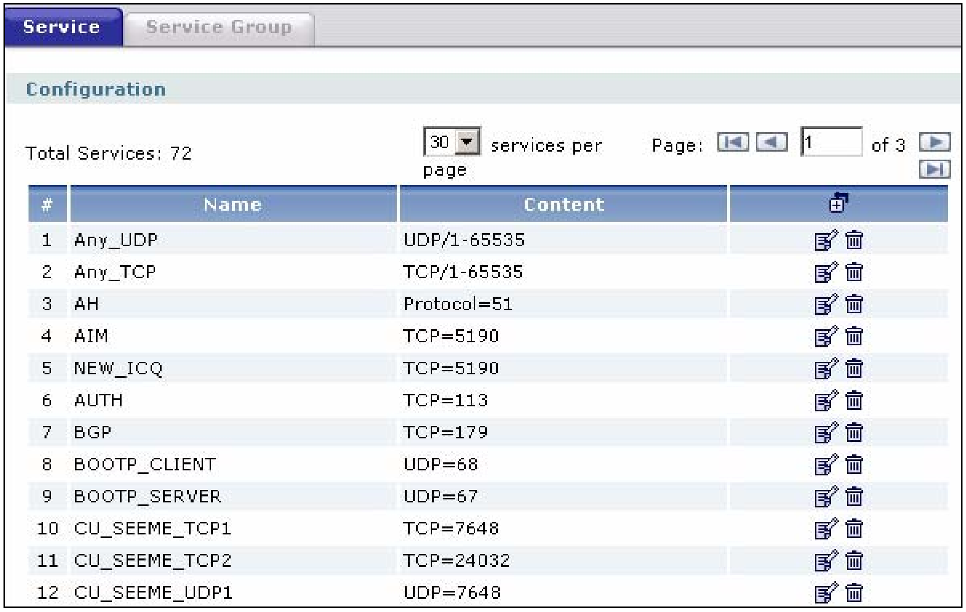
Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

36.2 Service Summary Screen

The **Service** summary screen provides a summary of all services and their definition. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the web configurator, and click **Object** > **Service** > **Service**.

Figure 382 Object > Service > Service



Total Services: 72

30 services per page

Page: 1 of 3

#	Name	Content
1	Any_UDP	UDP/1-65535
2	Any_TCP	TCP/1-65535
3	AH	Protocol=51
4	AIM	TCP=5190
5	NEW_ICQ	TCP=5190
6	AUTH	TCP=113
7	BGP	TCP=179
8	BOOTP_CLIENT	UDP=68
9	BOOTP_SERVER	UDP=67
10	CU_SEEME_TCP1	TCP=7648
11	CU_SEEME_TCP2	TCP=24032
12	CU_SEEME_UDP1	UDP=7648

The following table describes the labels in this screen.

Table 169 Object > Service > Service

LABEL	DESCRIPTION
Total Services	This displays the total number of services configured on the ZyWALL.
services per page	Select the number of services you want to appear per page here.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.

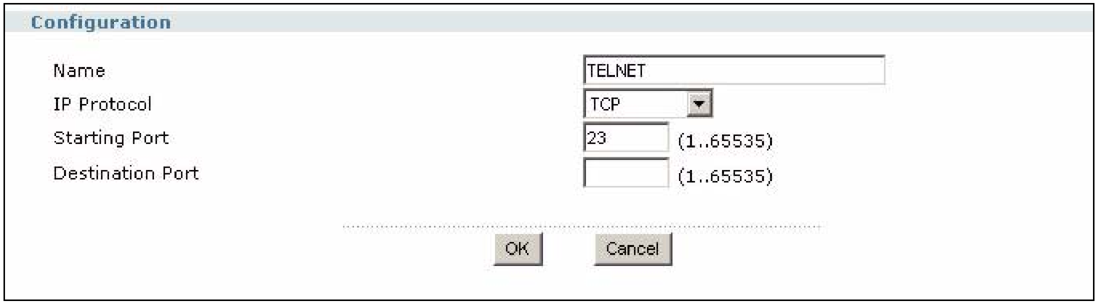
Table 169 Object > Service > Service (continued)

LABEL	DESCRIPTION
Content	This field displays a description of each service.
Add icon	This column provides icons to add, edit, and remove services. To add a service, click the **Add** icon at the top of the column. The **Service Add/ Edit** screen appears. To edit a service, click the **Edit** icon next to the service. The **Service Add/Edit** screen appears. To delete a service, click the **Remove** icon next to the service. The web configurator confirms that you want to delete the service before doing so.

36.2.1 Service Add/Edit

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see Section 36.2 on page 522), and click either the **Add** icon or an **Edit** icon.

Figure 383 Object > Service > Service > Edit



Configuration

Name: TELNET

IP Protocol: TCP

Starting Port: 23 (1..65535)

Destination Port: (1..65535)

The following table describes the labels in this screen.

Table 170 Object > Service > Service > Edit

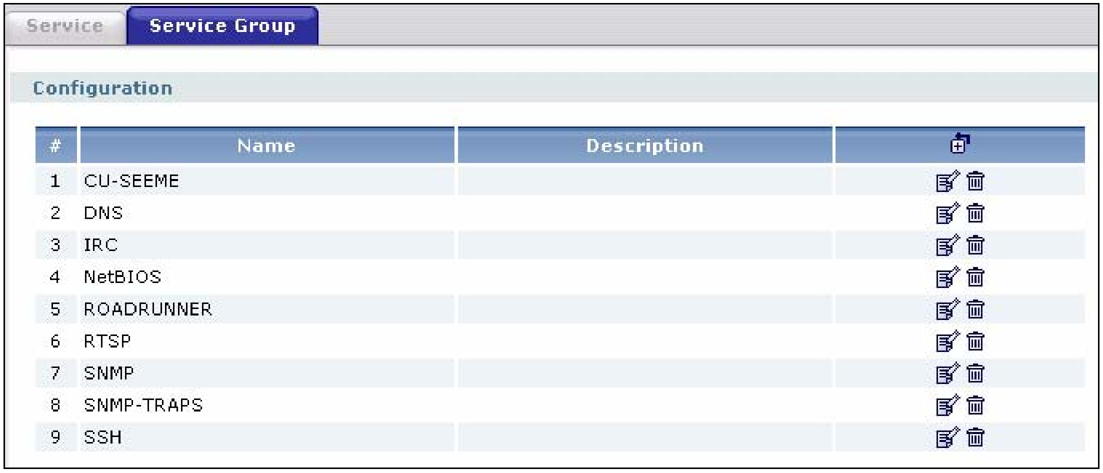
LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: **TCP**, **UDP**, **ICMP**, and **User Defined**.
Starting Port Ending Port	This field appears if the **IP Protocol** is **TCP** or **UDP**. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the **IP Protocol** is **ICMP Type**. Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the **IP Protocol** is **User Defined**. Enter the number of the next-level protocol (IP protocol). Allowed values are 0 - 255.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

36.3 Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the web configurator, and click **Object** > **Service** > **Service Group**.

Figure 384 Object > Service > Service Group



#	Name	Description	
1	CU-SEEME		
2	DNS		
3	IRC		
4	NetBIOS		
5	ROADRUNNER		
6	RTSP		
7	SNMP		
8	SNMP-TRAPS		
9	SSH		

The following table describes the labels in this screen. See Section 36.3.1 on page 524 for more information as well.

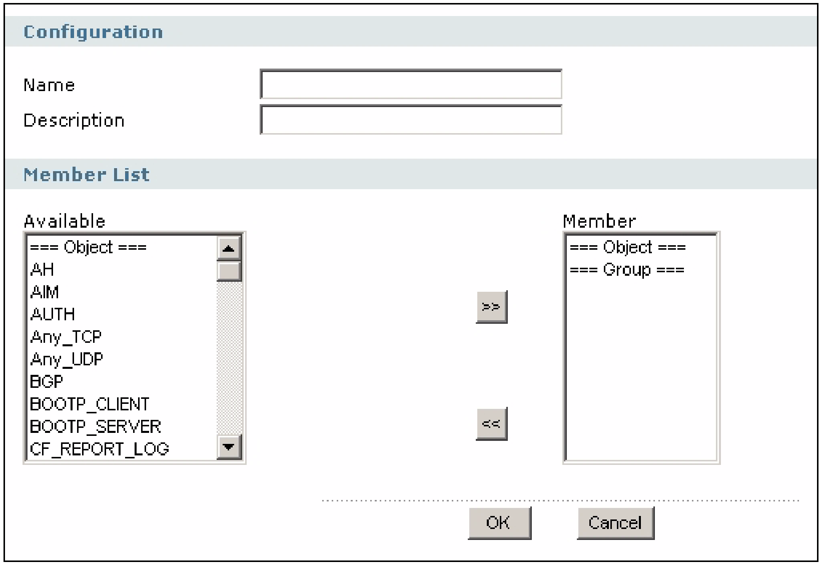
Table 171 Object > Service > Service Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific service group.
Name	This field displays the name of each service group.
Description	This field displays the description of each service group, if any.
Add icon	This column provides icons to add, edit, and remove service groups. To add a service group, click the **Add** icon at the top of the column. The **Service Group Add/Edit** screen appears. To edit a service group, click the **Edit** icon next to the service group. The **Service Group Add/Edit** screen appears. To delete a service group, click on the **Remove** icon next to the service group. The web configurator confirms that you want to delete the service group.

36.3.1 Service Group Add/Edit

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see Section 36.3 on page 524), and click either the **Add** icon or an **Edit** icon.

Figure 385 Object > Service > Service Group > Edit



Configuration
Name
Description
Member List
Available
=== Object ===
AH
AIM
AUTH
Any_TCP
Any_UDP
BGP
BOOTP_CLIENT
BOOTP_SERVER
CF_REPORT_LOG
>>
<<
Member
=== Object ===
=== Group ===
OK
Cancel

The following table describes the labels in this screen.

Table 172 Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Available	This field displays the names of the service and service group objects that can be added to the service group. Select service and service group objects that you want to be members of this group and click the right arrow to add them to the member list.
Member	This field displays the names of the service and service group objects that have been added to the service group. The order of members is not important. To remove members, select them and click the left arrow.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

37

Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering. See Section 5.5 on page 122 for related information on these screens.

37.1 Schedule Overview

The ZyWALL supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ZyWALL. See Section 43.3 on page 576 for information about the current date and time.

Schedules are based on the current date and time in the ZyWALL.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

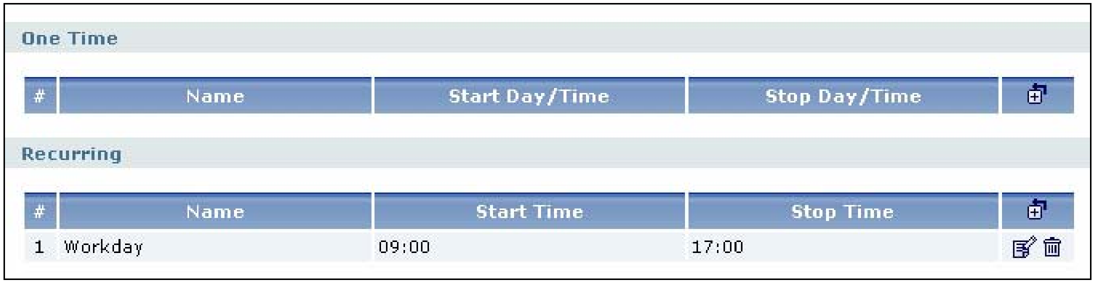
37.2 Schedule Screens

Use the **Schedule** summary screen and the **Schedule Add/Edit** screen to maintain schedules in the ZyWALL.

37.2.1 Schedule Summary

The **Schedule** summary screen provides a summary of all schedules in the ZyWALL. To access this screen, click **Object** > **Schedule**.

Figure 386 Object > Schedule



One Time

#	Name	Start Day/Time	Stop Day/Time	

Recurring

#	Name	Start Time	Stop Time	
1	Workday	09:00	17:00	

The following table describes the labels in this screen. See Section 37.2.2 on page 528 and Section 37.2.3 on page 529 for more information as well.

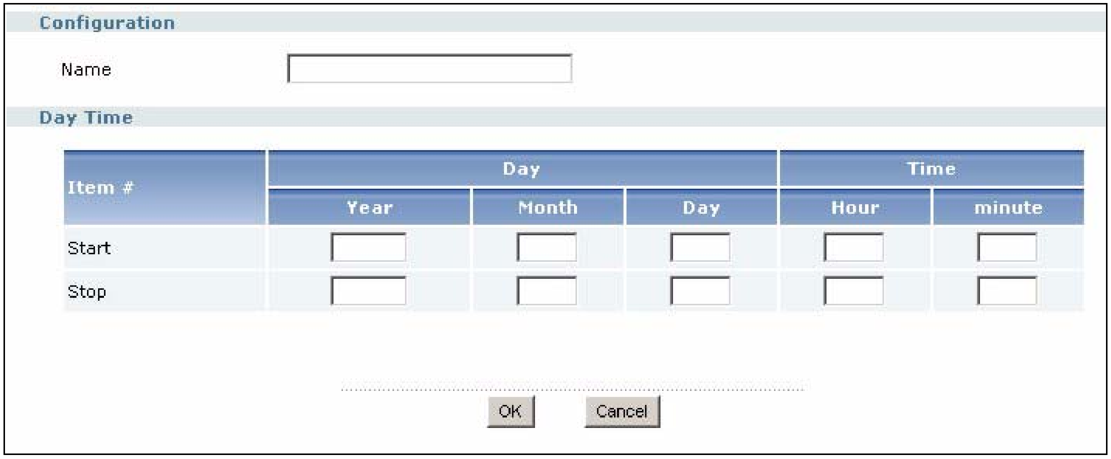
Table 173 Object > Schedule

LABEL	DESCRIPTION
One Time	
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Add icon	This column provides icons to add, edit, and remove schedules. To add a schedule, click the **Add** icon at the top of the column. The **Schedule Add/ Edit** screen appears. To edit a schedule, click the **Edit** icon next to the schedule. The **Schedule Add/ Edit** screen appears. To delete a schedule, click the **Remove** icon next to the schedule. The web configurator confirms that you want to delete the schedule before doing so.
Recurring	
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.
Add icon	This column provides icons to add, edit, and remove schedules. To add a schedule, click the **Add** icon at the top of the column. The **Schedule Add/ Edit** screen appears. To edit a schedule, click the **Edit** icon next to the schedule. The **Schedule Add/ Edit** screen appears. To delete a schedule, click the **Remove** icon next to the schedule. The web configurator confirms that you want to delete the schedule before doing so.

37.2.2 One-Time Schedule Add/Edit

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 37.2.1 on page 527), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 387 Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

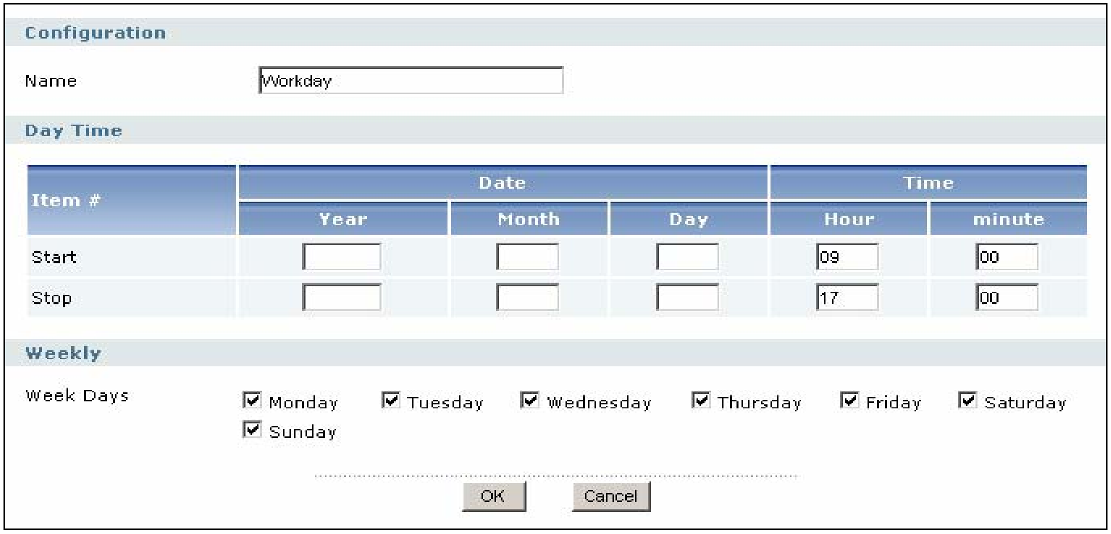
Table 174 Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
Start	Type the year, month, day, hour, and minute when the schedule begins. **Year** - 1900 - 2999 **Month** - 1 - 12 **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.) **Hour** - 0 - 23 **Minute** - 0 - 59 All of these fields are required.
Stop	Type the year, month, day, hour, and minute when the schedule ends. **Year** - 1900 - 2999 **Month** - 1 - 12 **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.) **Hour** - 0 - 23 **Minute** - 0 - 59 All of these fields are required.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

37.2.3 Recurring Schedule Add/Edit

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 37.2.1 on page 527), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 388 Object > Schedule > Edit (Recurring)



Name: Workday

Item #	Year	Month	Day	Hour	minute
Start				09	00
Stop				17	00

Week Days: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

Table 175 Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
Start	Type the hour and minute when the schedule begins each day. **Year** - disabled **Month** - disabled **Day** - disabled **Hour** - 0 - 23 **Minute** - 0 - 59 The **Hour** and **Minute** fields are both required. To set all day (24 hours), configure the start hour and minute both to 0.
Stop	Type the hour and minute when the schedule ends each day. **Year** - disabled **Month** - disabled **Day** - disabled **Hour** - 0 - 23 **Minute** - 0 - 59 The **Hour** and **Minute** fields are both required. To set all day (24 hours), configure the stop hour to 23 and minute to 59.
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

38

AAA Server

This chapter introduces and shows you how to configure the ZyWALL to use external authentication servers.

38.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the ZyWALL supports.

- Local user database

  The ZyWALL uses the built-in local user database to authenticate administrative users logging into the ZyWALL's web configurator or network access users logging into the network through the ZyWALL. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

38.1.1 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a ZyWALL OTP package in order to use this feature. The package contains server software and ZyWALL OTP tokens. Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1. Install the ASAS server software on a computer.
2. Create user accounts on the ZyWALL and in the ASAS server.
3. Import each token's database file (located on the included CD) into the server.
4. Assign users to OTP tokens (on the ASAS server).

5. Configure the ASAS as a RADIUS server in the ZyWALL's **Object > AAA Server** screens.
6. Give the OTP tokens to (local or remote) users.

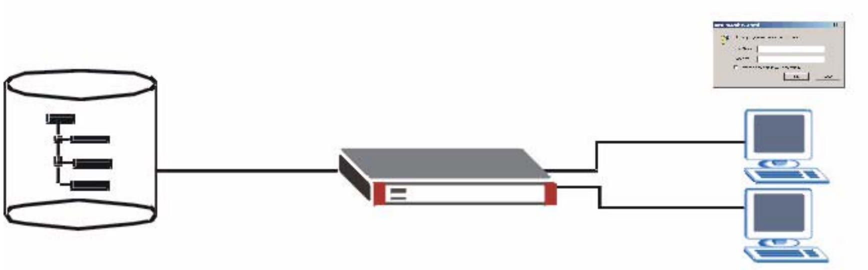
38.1.2 User Authentication Method

You can select to authenticate users using the local user database and/or a specified authentication server. By default, user accounts created and stored on the ZyWALL are authenticated locally.

38.2 Directory Service (AD/LDAP) Overview

LDAP/AD allows a client (the ZyWALL) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 389 Example: Directory Service Client and Server



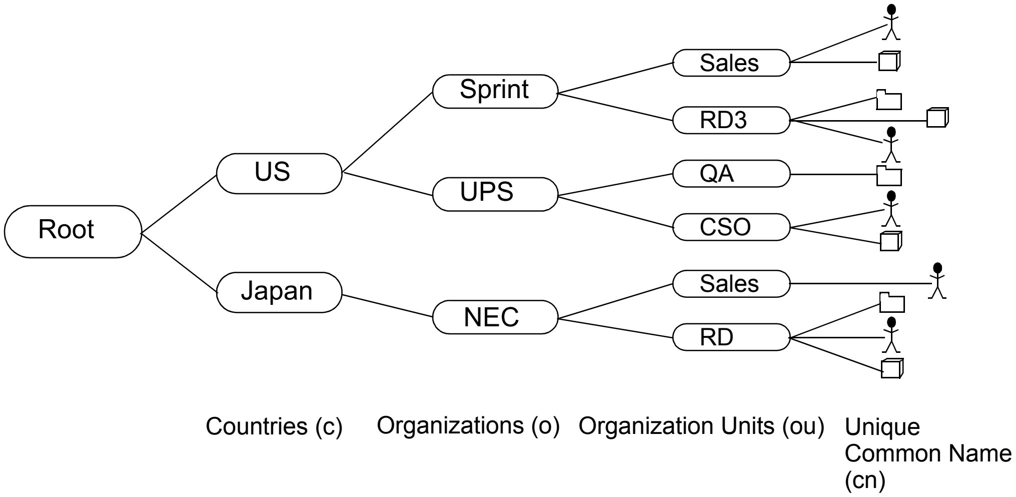
The following describes the user authentication procedure via an LDAP/AD server.

1. A user logs in with a user name and password pair.
2. The ZyWALL tries to bind (or log in) to the LDAP/AD server.
3. When the binding process is successful, the ZyWALL checks the user information in the directory against the user name and password pair.
4. If it matches, the user is allowed access. Otherwise, access is blocked.

38.2.1 Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 390 Basic Directory Structure



38.2.2 Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same “parent DN” (“`cn=domain1.com, ou=Sales, o=MyCompany`” in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

38.2.2.1 Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, `o=MyCompany`, `c=UK` where `o` means organization and `c` means country.

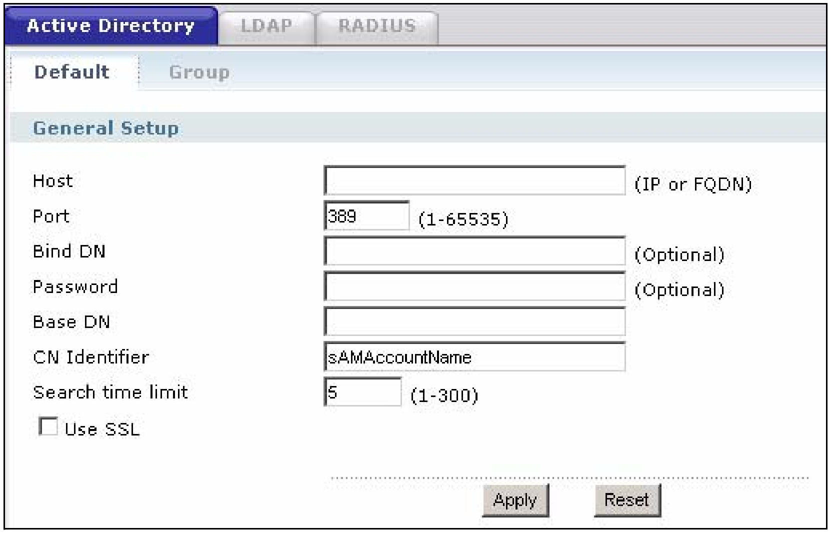
38.2.2.2 Bind DN

A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of `cn=zywallAdmin` allows the ZyWALL to log into the LDAP/AD server using the user name of `zywallAdmin`. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the ZyWALL will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

38.2.3 Configuring Active Directory or LDAP Default Server Settings

To configure the Active Directory or LDAP default server settings, click **Object > AAA Server > Active Directory** (or **LDAP**) to display the screen as shown.

Figure 391 Object > AAA Server > Active Directory (or LDAP) > Default



Host (IP or FQDN)

Port 389 (1-65535)

Bind DN (Optional)

Password (Optional)

Base DN

CN Identifier sAMAccountName

Search time limit 5 (1-300)

☐ Use SSL

The following table describes the labels in this screen.

Table 176 Object > AAA Server > Active Directory (or LDAP) > Default

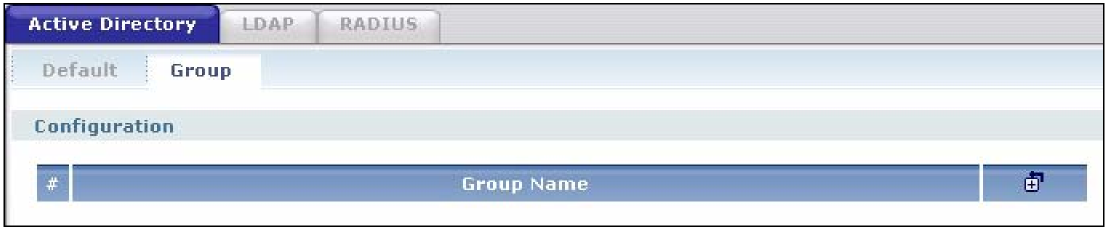
LABEL	DESCRIPTION
Host	Enter the IP address (in dotted decimal notation) or the fully-qualified domain name (up to 63 alphanumerical characters) of an AD or LDAP server.
Port	Specify the port number on the AD or LDAP server to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535. The default is **389**.
Bind DN	Specify the bind DN for logging into the LDAP server. Enter up to 63 alphanumerical characters. For example, `cn=zywallAdmin` specifies `zywallAdmin` as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the ZyWALL to bind (or log in) to the AD or LDAP server.
Base DN	Specify the directory (up to 63 alphanumerical characters). For example, `o=ZyXEL, c=US`.
CN Identifier	Specify the unique common name that uniquely identifies a record in the AD or LDAP directory. Enter up to 63 alphanumerical characters.
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the AD or LDAP server. In this case, user authentication fails. The search timeout occurs when either the user information is not in the LDAP server or the server is down.
Use SSL	Select **Use SSL** to establish a secure connection to the AD or LDAP server.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to start configuring this screen again.

38.3 Active Directory or LDAP Group Summary

You can configure a group of AD or LDAP servers in the **Active Directory** (or **LDAP**) > **Group** screen. This is useful if you have more than one AD server or more than one LDAP server for user authentication in a network. You can create up to 16 AD server groups with up to four members in each group on the ZyWALL. You can also create up to 16 LDAP server groups with up to four members in each group on the ZyWALL.

1 Click **Object** > **AAA Server** > **Active Directory** (or **LDAP**) > **Group** to display the screen.

Figure 392 Object > AAA Server > Active Directory (or LDAP) > Group


Active Directory
LDAP
RADIUS
Default
Group
Configuration
#
Group Name

The following table describes the labels in this screen.

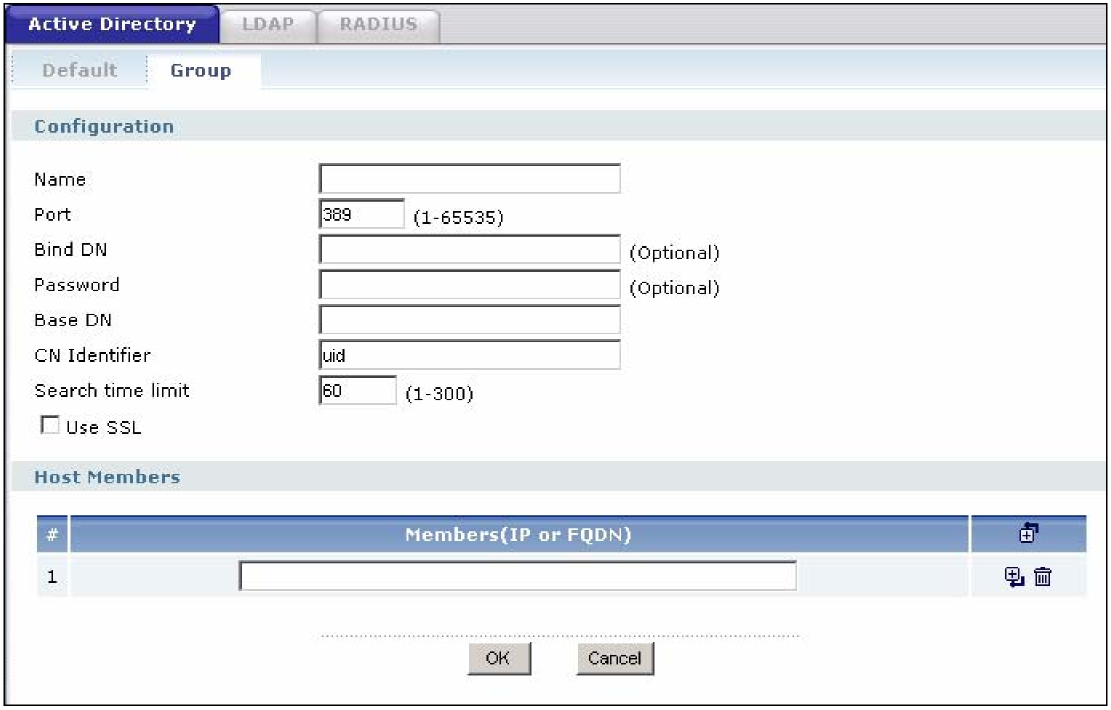
Table 177 Object > AAA Server > Active Directory (or LDAP) > Group

LABEL	DESCRIPTION
#	This field displays the index number.
Group Name	This field displays the descriptive name for identification purposes.
Add icon	Click **Add** to add a new entry. Click **Edit** to edit the settings of an entry. Click **Delete** to remove an entry.

2 Click the **Add** icon or an **Edit** icon to display the configuration fields.

38.3.1 Creating an Active Directory or LDAP Group

Figure 393 Object > AAA Server > Active Directory (or LDAP) > Group > Add


Active Directory
LDAP
RADIUS
Default
Group
Configuration

Name
Port 389 (1-65535)
Bind DN (Optional)
Password (Optional)
Base DN
CN Identifier uid
Search time limit 60 (1-300)
☐ Use SSL

Host Members
#
Members(IP or FQDN)
1
OK
Cancel

The following table describes the labels in this screen.

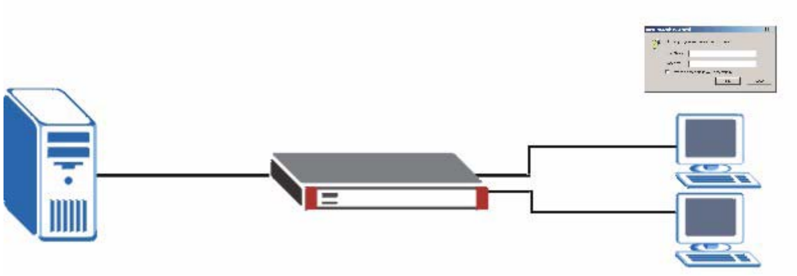
Table 178 Object > AAA Server > Active Directory (or LDAP) > Group > Add

LABEL	DESCRIPTION
Configuration	All AD or LDAP servers in a group share the same settings in the fields below.
Name	Enter a descriptive name (up to 63 alphanumerical characters). for identification purposes.
Port	Specify the port number on the LDAP server(s) to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.
Password	If required, enter the password (up to 15 alphanumerical characters) the ZyWALL uses to log into the AD or LDAP server(s).
Base DN	Specify the top level directory in the directory. For example, `o=ZyXEL, c=US`.
binddn	Specify the bind DN for logging into the AD or LDAP server(s). For example, `cn=zywallAdmin` specifies `zywallAdmin` as the user name.
CN Identifier	Specify the unique common name that uniquely identifies a record in the AD or LDAP directory. Enter up to 63 alphanumerical characters.
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Use SSL	Select **Use SSL** to establish a secure connection to the AD or LDAP server(s).
Host Members	The ordering of the LDAP servers is important as the ZyWALL uses the AD or LDAP servers for user authentication in the order they appear in this table.
#	This field displays the index number.
Members	Specify the URI (Uniform Resource Identifier) of an AD or LDAP server. You can enter the IP address (in dotted decimal notation) or the fully qualified domain name (FQDN; up to 63 alphanumerical characters) of the AD or LDAP server.
Add icon	Click **Add** to add a new AD or LDAP server. You can add up to four AD or LDAP member servers. Click **Delete** to remove an AD or LDAP server.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

38.4 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

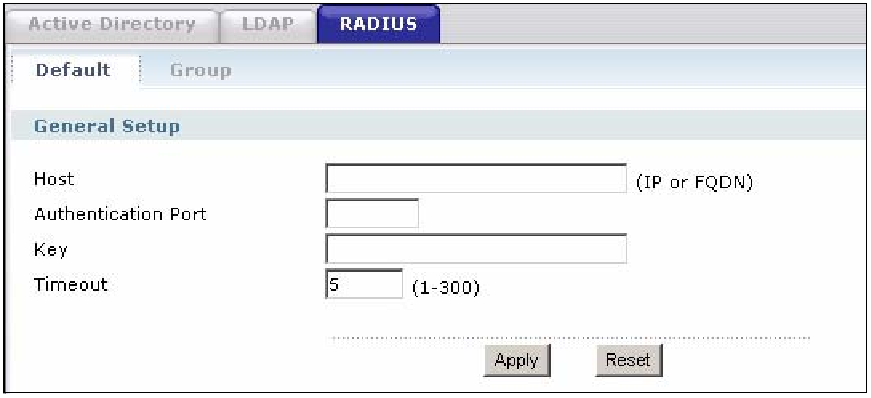
Figure 394 RADIUS Server Network Example



38.5 Configuring a Default RADIUS Server

To configure the default external RADIUS server to use for user authentication, click **Object** > **AAA Server** > **RADIUS** to display the screen as shown.

Figure 395 Object > AAA Server > RADIUS > Default



Host (IP or FQDN)
Authentication Port
Key
Timeout 5 (1-300)

The following table describes the labels in this screen.

Table 179 Object > AAA Server > RADIUS > Default

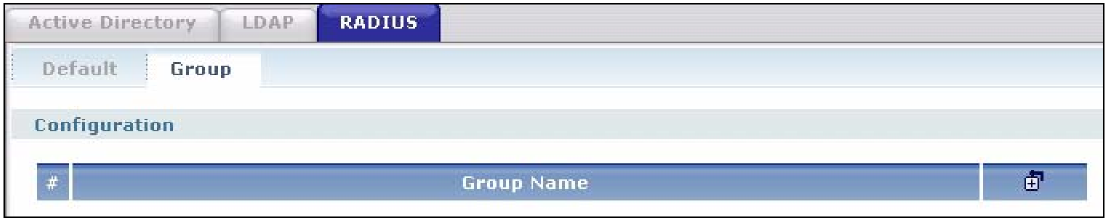
LABEL	DESCRIPTION
Host	Enter the IP address (in dotted decimal notation) or the domain name (up to 63 alphanumeric characters) of a RADIUS server.
Authentication Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and the ZyWALL.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to start configuring this screen again.

38.6 Configuring a Group of RADIUS Servers

You can configure a group of RADIUS servers in the **RADIUS** > **Group** screen. This is useful if you have more than one authentication server for user authentication in a network.

1 Click **Object** > **AAA Server** > **RADIUS** > **Group** to display the screen.

Figure 396 Object > AAA Server > RADIUS > Group


Active Directory
LDAP
RADIUS
Default
Group
Configuration
#
Group Name

The following table describes the labels in this screen.

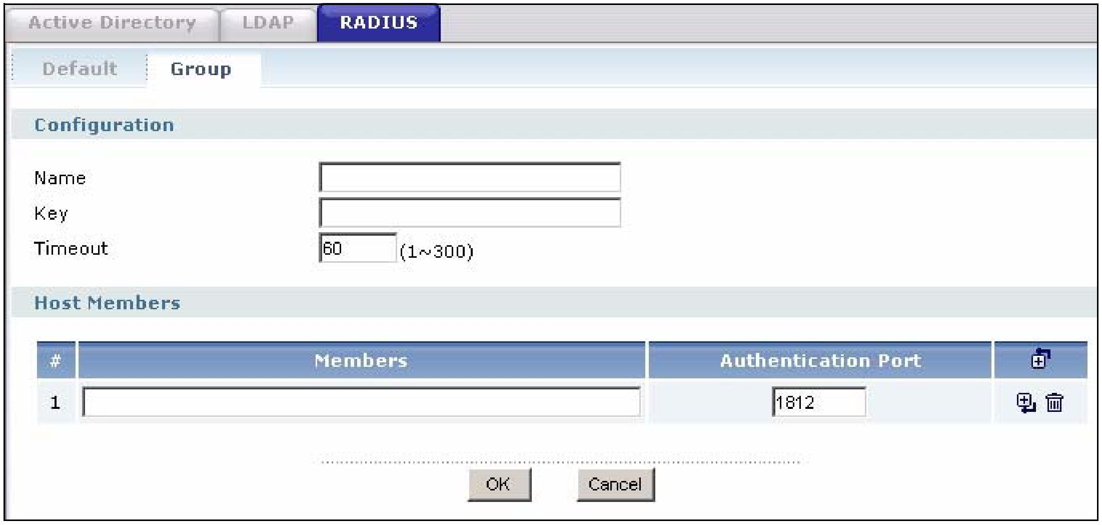
Table 180 Object > AAA Server > RADIUS > Group

LABEL	DESCRIPTION
#	This field displays the index number.
Group Name	This field displays the descriptive name for identification purposes.
Add icon	Click **Add** to add a new entry. Click **Edit** to edit the settings of an entry. Click **Delete** to remove an entry.

2 Click the **Add** icon or an **Edit** icon to display the configuration fields.

38.6.1 Adding a RADIUS Server Member

Figure 397 Object > AAA Server > RADIUS > Group > Add


Active Directory
LDAP
RADIUS
Default
Group
Configuration
Name
Key
Host Members
#
Members
Authentication Port
OK
Cancel

Timeout 60 (1~300)

1 Authentication Port 1812

The following table describes the labels in this screen.

Table 181 Object > AAA Server > RADIUS > Group > Add

LABEL	DESCRIPTION
Configuration	All RADIUS servers in a group share the same settings in the fields below.
Name	Enter a descriptive name (up to 63 alphanumeric characters) for identification purposes.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and the ZyWALL.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Host Members	The ordering of the RADIUS servers is important as the ZyWALL uses the RADIUS servers for user authentication in the order they appear in this table.
#	This field displays the index number.
Members	Enter the IP address (in dotted decimal notation) or the domain name (up to 63 alphanumeric characters) of a RADIUS server.
Authentication Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Add icon	Click **Add** to add a new RADIUS server. You can add up to four RADIUS member servers. Click **Delete** to remove a RADIUS server.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

39.1 Authentication Objects Overview

After you have created the AAA server objects in the **AAA Server** screens, you can specify the authentication objects (containing the AAA server information) that the ZyWALL uses to authenticate users (using VPN or managing through HTTP/HTTPS).

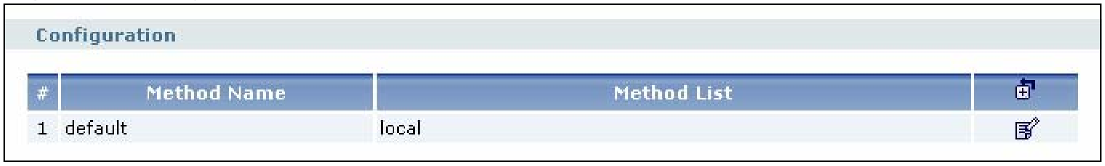
Specify the authentication server(s) and/or server group(s) in the **Auth. Method** screen to create an authentication object.

39.2 Viewing Authentication Objects

Click **Object** > **Auth. Method** to display the screen as shown.

You can create up to 16 authentication objects.

Figure 398 Object > Auth. Method



#	Method Name	Method List
1	default	local

The following table describes the labels in this screen.

Table 182 Object > Auth. Method

LABEL	DESCRIPTION
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.
Add icon	Click **Add** to add a new entry. Click **Edit** to edit the settings of an entry. Click **Delete** to remove an entry.

39.3 Creating an Authentication Object

Follow the steps below to create an authentication object.

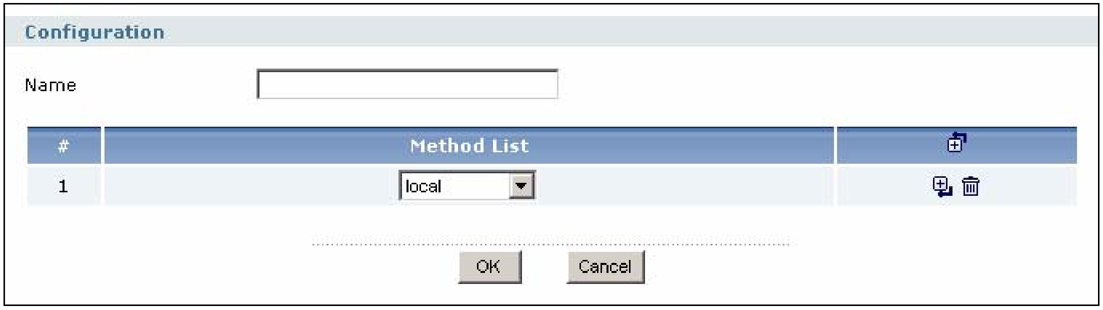
1. Click **Object** > **Auth. Method**.
2. Click **Add**.
3. Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.
4. Click **Add** to insert an authentication method in the table.
5. Select a server object from the **Method List** drop-down list box.
6. You can add up to four server objects to the table. The ordering of the **Method List** column is important. The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

   If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn’t match the one on the first authentication server.

You can NOT select two server objects of the same type.

7. Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 399 Object > Auth. Method > Add



The following table describes the labels in this screen.

Table 183 Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.
Method List	Select a server object from the drop-down list box. You can create a server object in the **AAA Server** screen (see Chapter 38 on page 531 for more information). The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn’t match the one on the first authentication server.
Add icon	Click **Add** to add a new entry. Click **Edit** to edit the settings of an entry. Click **Delete** to delete an entry.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

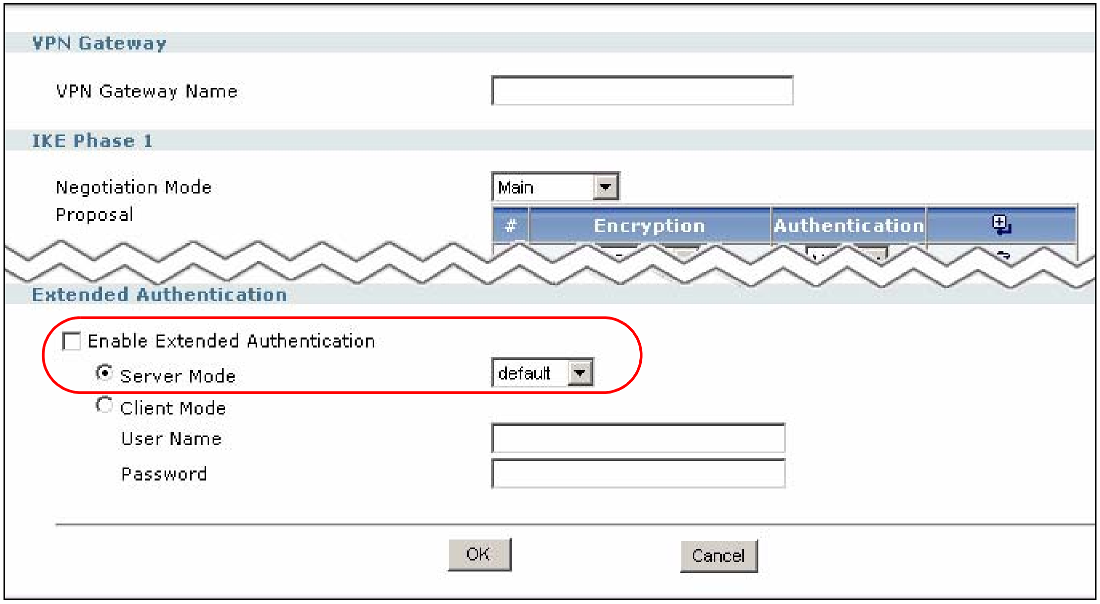
39.3.1 Example: Selecting a VPN Authentication Method

After you set up an authentication method in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

1. Access the **VPN > IPSec VPN > VPN Gateway** > **Edit** screen.
2. Select **Enable Extended Authentication**.
3. Select **Server Mode** and select an authentication method object from the drop-down list box.
4. Click **OK** to save the settings.

Figure 400 Example: Using Authentication Method in VPN



VPN Gateway

VPN Gateway Name

IKE Phase 1

Negotiation Mode: Main

Proposal

#	Encryption	Authentication

Extended Authentication

☐ Enable Extended Authentication

● Server Mode: default

○ Client Mode

User Name

Password

40

Certificates

This chapter gives background information about public-key certificates and explains how to use the **Certificates** screens. See Section 5.5 on page 122 for related information on these screens.

40.1 Certificates Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyWALL does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyWALL can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

40.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyWALL only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

40.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the ZyWALL act as a certification authority and sign its own certificates.

40.3 Factory Default Certificate

The ZyWALL generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

40.3.1 Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The ZyWALL currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it decrypt the contents when you import the file into the ZyWALL.

Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

40.4 Certificate Configuration Screens Summary

This section summarizes how to manage certificates on the ZyWALL.

Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.

Use the **Trusted Certificates** screens to save CA certificates and trusted remote host certificates to the ZyWALL. The ZyWALL will trust any valid certificate that you have imported as a trusted certificate. It will also trust any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

40.5 Verifying a Certificate

Before you import a certificate into the ZyWALL, you should verify that you have the actual certificate. This is especially true of trusted certificates since the ZyWALL also trusts any valid certificate signed by any of the imported trusted certificates.

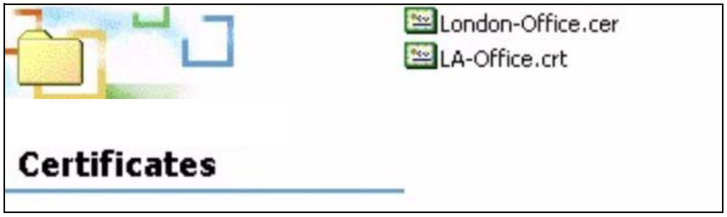
40.5.1 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

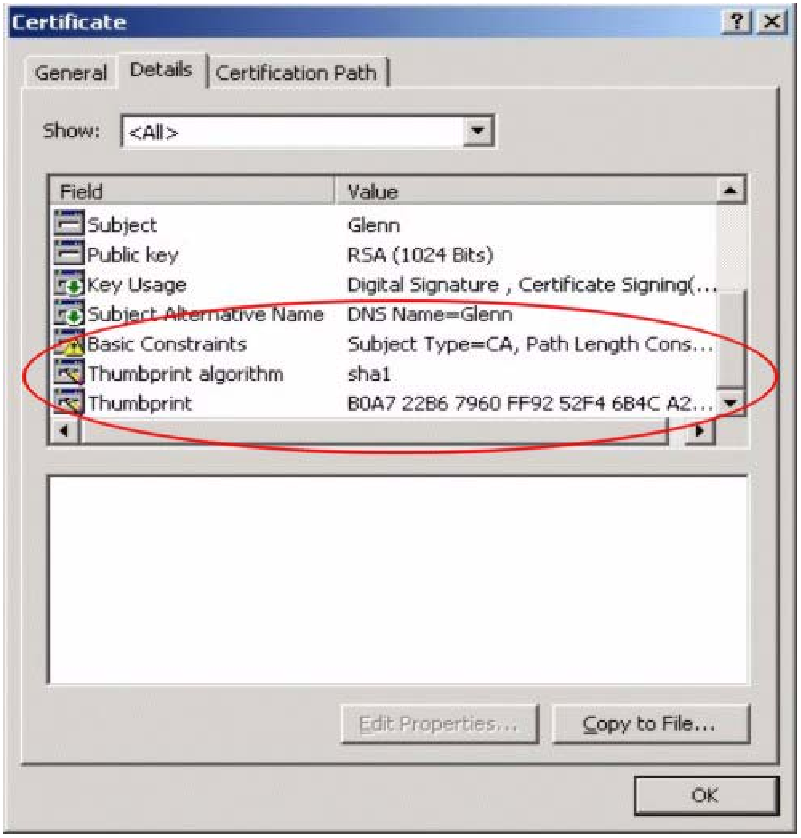
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 401 Remote Host Certificates



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 402 Certificate Details


Certificate
General
Details
Certification Path
Edit Properties...
Copy to File...
OK

Show: <All>

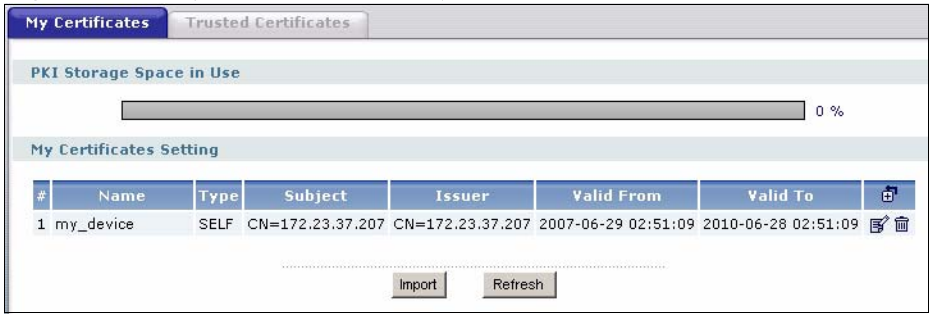
Field	Value
Subject	Glenn
Public key	RSA (1024 Bits)
Key Usage	Digital Signature , Certificate Signing(...
Subject Alternative Name	DNS Name=Glenn
Basic Constraints	Subject Type=CA, Path Length Cons...
Thumbprint algorithm	sha1
Thumbprint	B0A7 22B6 7960 FF92 52F4 6B4C A2...

4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

40.6 My Certificates Screen

Click **Object** > **Certificate** > **My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests.

Figure 403 Object > Certificate > My Certificates


My Certificates
Trusted Certificates
Import
Refresh

PKI Storage Space in Use

0 %

My Certificates Setting

#	Name	Type	Subject	Issuer	Valid From	Valid To	
1	my_device	SELF	CN=172.23.37.207	CN=172.23.37.207	2007-06-29 02:51:09	2010-06-28 02:51:09	

The following table describes the labels in this screen.

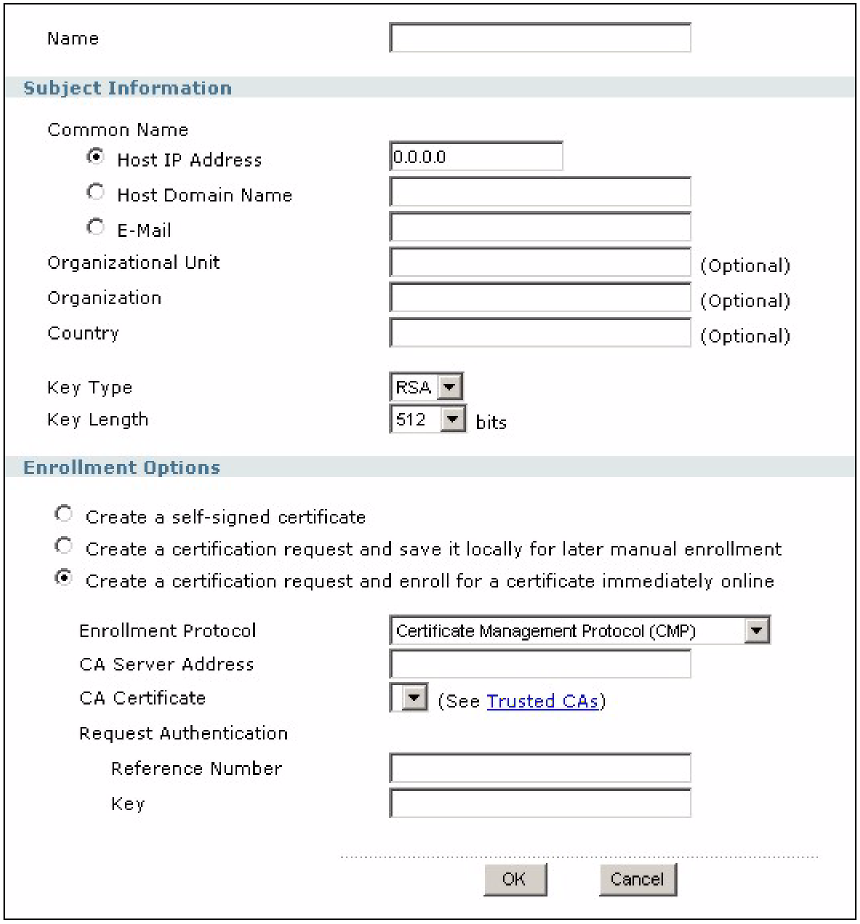
Table 184 Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Add icon	Click the **Add** icon to go to the screen where you can have the ZyWALL generate a certificate or a certification request. Click the **Edit** icon to open a screen with an in-depth list of information about the certificate. The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. Click the **Delete** icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificate. Subsequent certificates move up by one when you take this action. You cannot delete certificates that any of the ZyWALL's features are configured to use.
Import	Click **Import** to open a screen where you can save a certificate to the ZyWALL.
Refresh	Click **Refresh** to display the current validity status of the certificates.

40.6.1 My Certificates Add Screen

Click **Object** > **Certificate** > **My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the ZyWALL create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 404 Object > Certificate > My Certificates > Add



Name

Subject Information

Common Name
● Host IP Address 0.0.0.0
○ Host Domain Name
○ E-Mail
Organizational Unit (Optional)
Organization (Optional)
Country (Optional)

Key Type RSA
Key Length 512 bits

Enrollment Options

○ Create a self-signed certificate
○ Create a certification request and save it locally for later manual enrollment
● Create a certification request and enroll for a certificate immediately online

Enrollment Protocol Certificate Management Protocol (CMP)
CA Server Address
CA Certificate (See Trusted CAs)
Request Authentication
Reference Number
Key

The following table describes the labels in this screen.

Table 185 Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate’s owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 185 Object > Certificate > My Certificates > Add (continued)

LABEL	DESCRIPTION
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select **RSA** to use the Rivest, Shamir and Adleman public-key algorithm. Select **DSA** to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyWALL generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 40.6.2 on page 552) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the ZyWALL generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server. For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/ :.=?;!*#@$_%-
CA Certificate	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. Click **Trusted CAs** to go to the **Trusted Certificates** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities.

Table 185 Object > Certificate > My Certificates > Add (continued)

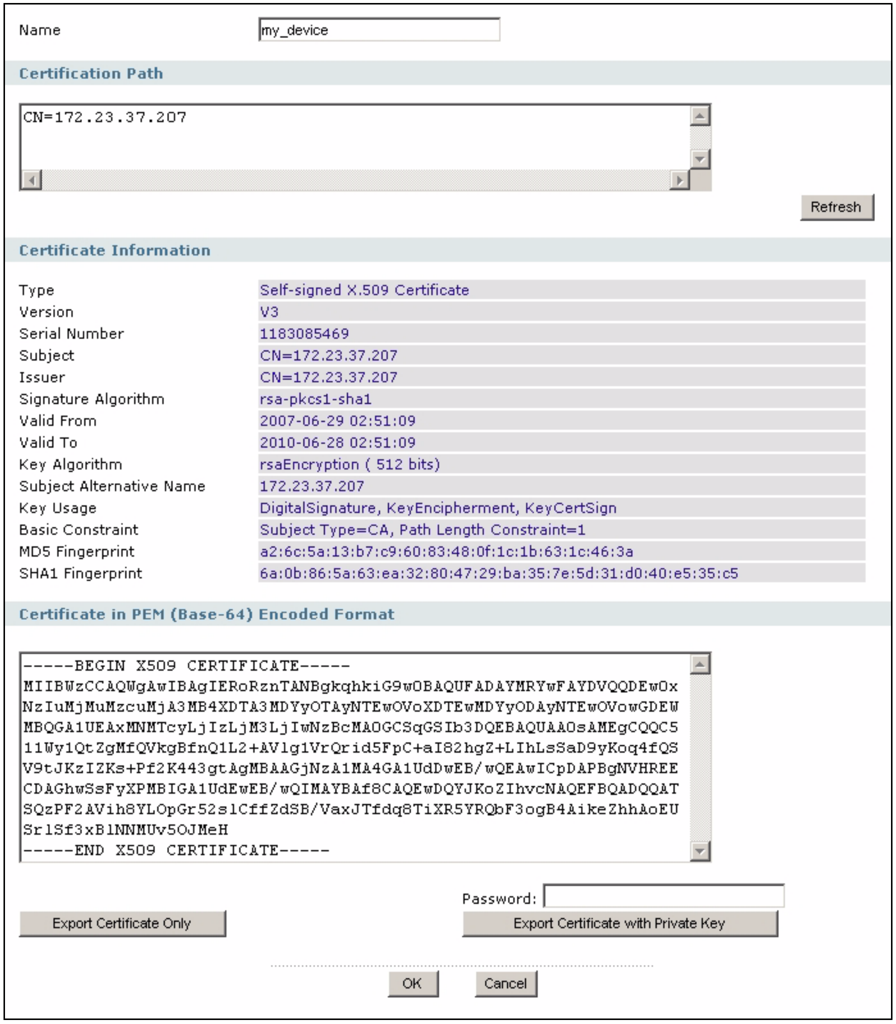
LABEL	DESCRIPTION
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol. For the reference number, use 0 to 99999999. For the key, use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyWALL enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyWALL to enroll a certificate online.

40.6.2 My Certificate Edit Screen

Click **Object** > **Certificate** > **My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 405 Object > Certificate > My Certificates > Edit



Name	my_device

Certification Path

```
CN=172.23.37.207
```

Certificate Information

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	1183085469
Subject	CN=172.23.37.207
Issuer	CN=172.23.37.207
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2007-06-29 02:51:09
Valid To	2010-06-28 02:51:09
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	172.23.37.207
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	a2:6c:5a:13:b7:c9:60:83:48:0f:1c:1b:63:1c:46:3a
SHA1 Fingerprint	6a:0b:86:5a:63:ea:32:80:47:29:ba:35:7e:5d:31:d0:40:e5:35:c5

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIBWzCCAQWgAwIBAgIERoRznTANBgkqhkiG9w0BAQUFADAYMRYwFAYDVQQDEw0x
NzIuMjMuMzcuMjA3MB4XDTA3MDYyOTAyNTEwOVoXDTEwMDYyODAyNTEwOVowGDEW
MBQGA1UEAxMNMTcyLjIzLjM3LjIwNzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC5
11Wy1QtZgMfQVkgBfnQ1L2+AVlg1VrQrid5FpC+aI82hgZ+LIhLsSaD9yKoq4fQS
V9tJKzIZKs+Pf2K443gtAgMBAAGjNzA1MA4GA1UdDwEB/wQEAwICpDAPBgNVHREE
CDAGhwSsFyXPMBIGA1UdEwEB/wQIMAYBAf8CAQEwDQYJKoZIhvcNAQEFBQADQQAT
SQzPF2AVih8YLOpGr52slCffZdSB/VaxJTfdq8TiXR5YRQbF3ogB4AikeZhhAoEU
Sr1Sf3xBlNNMUv5OJMeH
-----END X509 CERTIFICATE-----
```

The following table describes the labels in this screen.

Table 186 Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyWALL does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.

Table 186 Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number. "
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyWALL.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyWALL uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).

Table 186 Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Export	This button displays for a certification request. Use this button to save a copy of the request without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the ZyWALL. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

40.6.3 My Certificate Import Screen

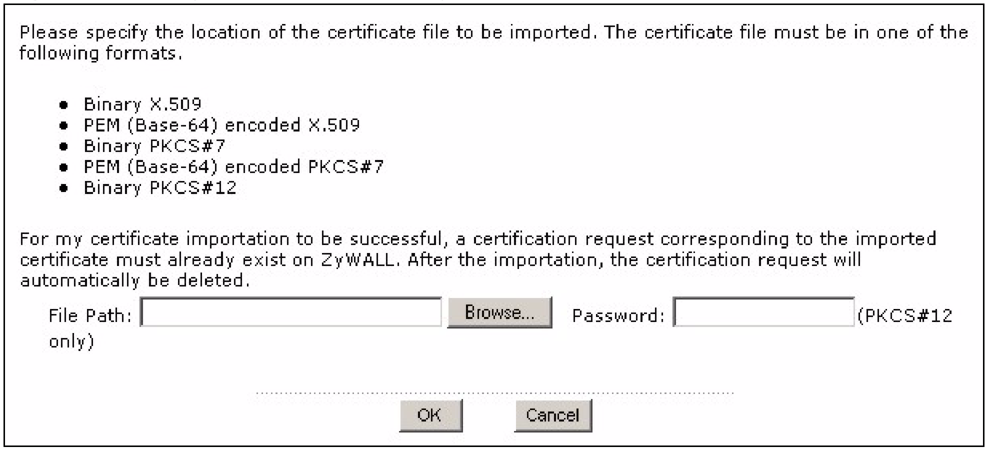
Click **Object** > **Certificate** > **My Certificates** > **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyWALL.

> You can import a certificate that matches a corresponding certification request that was generated by the ZyWALL. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 406 Object > Certificate > My Certificates > Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7
- Binary PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.

File Path: Password: (PKCS#12 only)

The following table describes the labels in this screen.

Table 187 Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the ZyWALL.
Browse	Click **Browse** to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

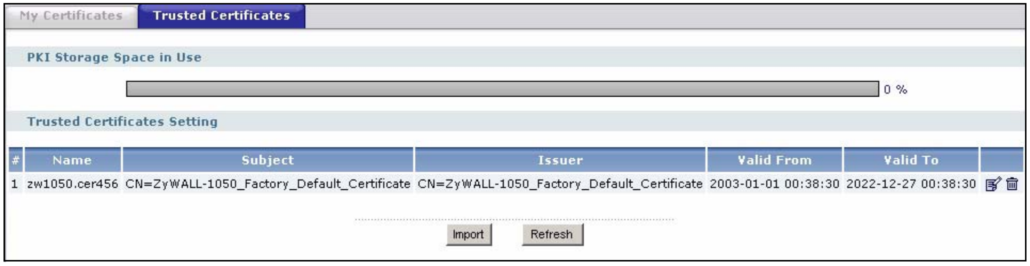
40.7 Trusted Certificates Screen

Click **Object** > **Certificate** > **Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the ZyWALL to accept as trusted. The ZyWALL also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

40.7.1 OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the ZyWALL checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the ZyWALL only gets information on the certificates that it needs to verify, not a huge list. When the ZyWALL requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

Figure 407 Object > Certificate > Trusted Certificates



#	Name	Subject	Issuer	Valid From	Valid To	
1	zw1050.cer456	CN=ZyWALL-1050_Factory_Default_Certificate	CN=ZyWALL-1050_Factory_Default_Certificate	2003-01-01 00:38:30	2022-12-27 00:38:30	

The following table describes the labels in this screen.

Table 188 Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.

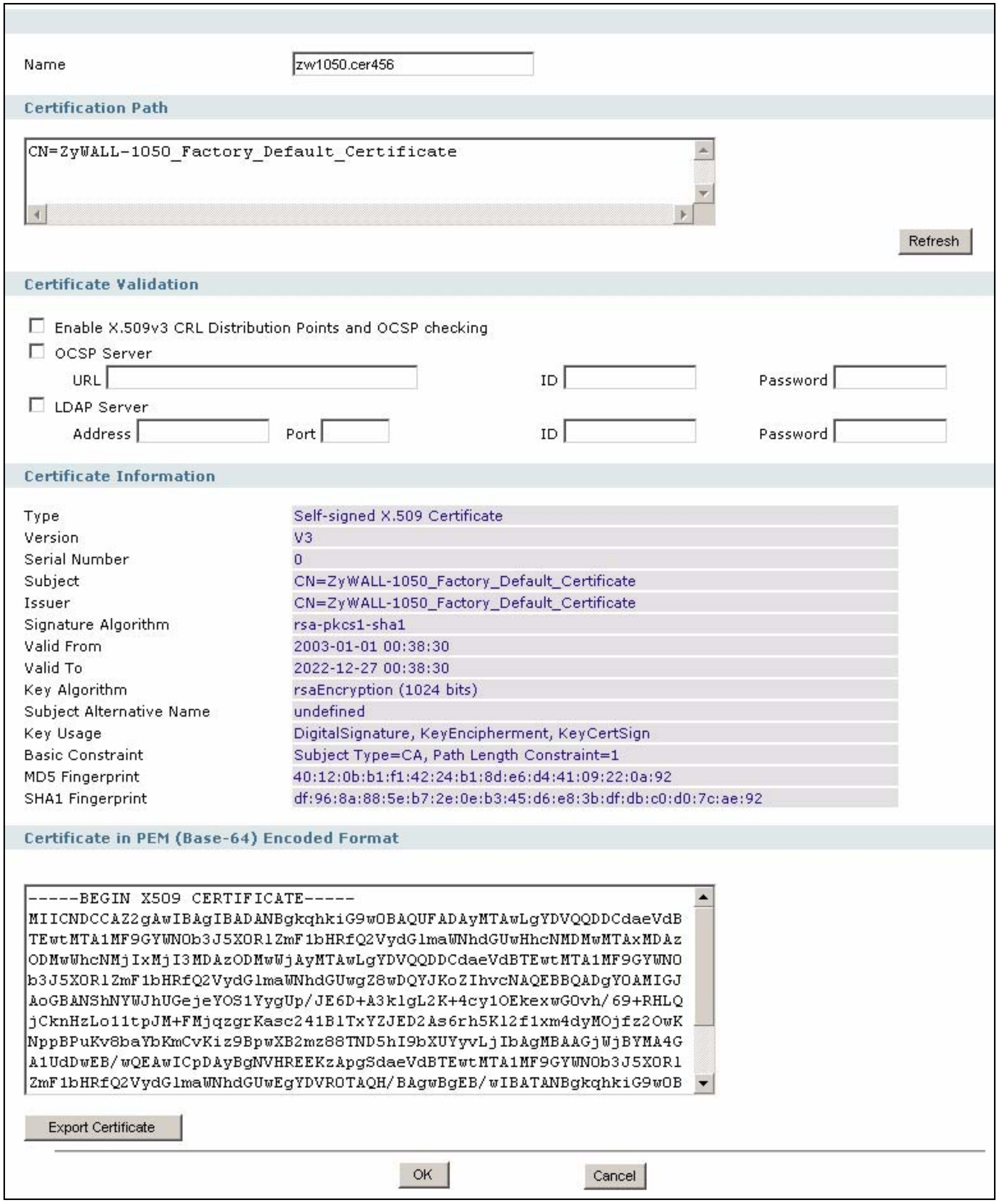
Table 188 Object > Certificate > Trusted Certificates (continued)

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
(icons)	Click the **Edit** icon to open a screen with an in-depth list of information about the certificate. The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. Click the **Delete** icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyWALL.
Refresh	Click this button to display the current validity status of the certificates.

40.8 Trusted Certificates Edit Screen

Click **Object** > **Certificate** > **Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the ZyWALL to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 408 Object > Certificate > Trusted Certificates > Edit



Name: zw1050.cer456

Certification Path

```
CN=ZyWALL-1050_Factory_Default_Certificate
```

Refresh
Certificate Validation
☐ Enable X.509v3 CRL Distribution Points and OCSP checking
☐ OCSP Server
URL
ID
Password
☐ LDAP Server
Address
Port
ID
Password
Certificate Information

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	0
Subject	CN=ZyWALL-1050_Factory_Default_Certificate
Issuer	CN=ZyWALL-1050_Factory_Default_Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2003-01-01 00:38:30
Valid To	2022-12-27 00:38:30
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	undefined
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	40:12:0b:b1:f1:42:24:b1:8d:e6:d4:41:09:22:0a:92
SHA1 Fingerprint	df:96:8a:88:5e:b7:2e:0e:b3:45:d6:e8:3b:df:db:c0:d0:7c:ae:92

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIICNDCCAZ2gAwIBAgIBADANBgkqhkiG9w0BAQUFADAyMTAwLgYDVQQDDCdaeVdB
TEwtMTA1MF9GYWN0b3J5X0RlZmF1bHRfQ2VydGlmaWNhdGUwHhcNMDMwMTAxMDAz
ODMwWhcNMjIxMjI3MDAzODMwWjAyMTAwLgYDVQQDDCdaeVdBTEwtMTA1MF9GYWN0
b3J5X0RlZmF1bHRfQ2VydGlmaWNhdGUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBANShNYWJhUGejeYOS1YygUp/JE6D+A3klgL2K+4cy1OEkexwGOvh/69+RHLQ
jCknHzLo11tpJM+FMjqzgrKasc241BlTxYZJED2As6rh5Kl2f1xm4dyMOjfz2OwK
NppBPuKv8baYbKmCvKiz9BpwXB2mz88TND5hI9bXUYyvLjIbAgMBAAGjWjBYMA4G
A1UdDwEB/wQEAwICpDAyBgNVHREEKzApgSdaeVdBTEwtMTA1MF9GYWN0b3J5X0Rl
ZmF1bHRfQ2VydGlmaWNhdGUwEgYDVR0TAQH/BAgwBgEB/wIBATANBgkqhkiG9w0B
```

Export Certificate
OK
Cancel

The following table describes the labels in this screen.

Table 189 Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyWALL does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.

Table 189 Object > Certificate > Trusted Certificates > Edit (continued)

LABEL	DESCRIPTION
Refresh	Click **Refresh** to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to have the ZyWALL check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The ZyWALL may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The ZyWALL may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).

Table 189 Object > Certificate > Trusted Certificates > Edit (continued)

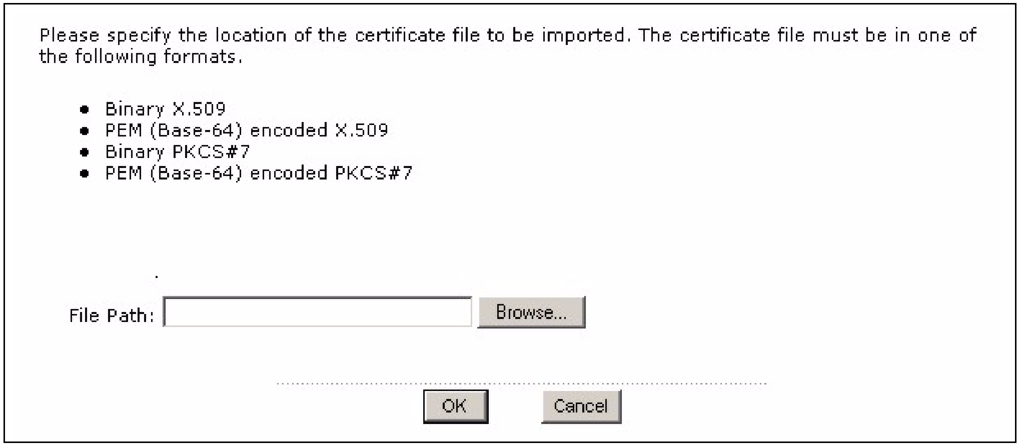
LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the ZyWALL. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

40.9 Trusted Certificates Import Screen

Click **Object** > **Certificate** > **Trusted Certificates** > **Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the ZyWALL.

You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 409 Object > Certificate > Trusted Certificates > Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

The following table describes the labels in this screen.

Table 190 Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the ZyWALL.
Browse	Click **Browse** to find the certificate file you want to upload.
OK	Click **OK** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the previous screen.

41

ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. See Section 5.5 on page 122 for related information on these screens.

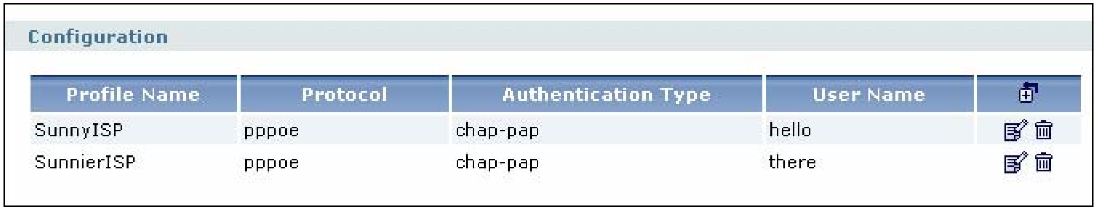
41.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE or PPTP. See Section 10.6 on page 210 for information about PPPoE/PPTP interfaces.

41.2 ISP Account Summary

This screen provides a summary of ISP accounts in the ZyWALL. To access this screen, click **Object** > **ISP Account**.

Figure 410 Object > ISP Account



Profile Name	Protocol	Authentication Type	User Name	
SunnyISP	pppoe	chap-pap	hello	
SunnierISP	pppoe	chap-pap	there	

The following table describes the labels in this screen. See the ISP Account Edit section below for more information as well.

Table 191 Object > ISP Account

LABEL	DESCRIPTION
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.

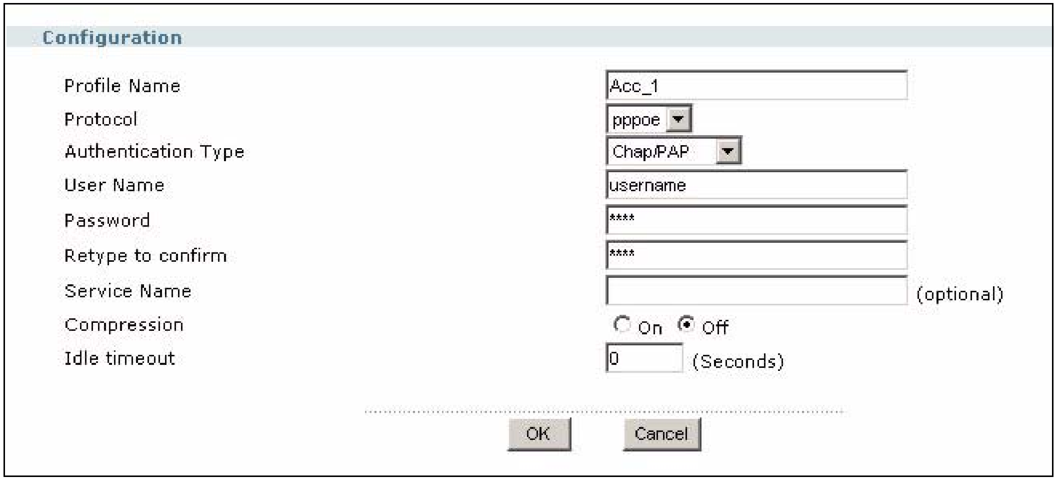
Table 191 Object > ISP Account (continued)

LABEL	DESCRIPTION
User Name	This field displays the user name of the ISP account.
Add icon	This column provides icons to add, edit, and remove ISP accounts. To add information about a new ISP account, click the **Add** icon at the top of the column. The **ISP Account Edit** screen appears. To edit information about an existing account, click the **Edit** icon next to the ISP account. The **ISP Account Edit** screen appears. To remove information about an existing account, click the **Remove** icon next to the ISP account. The web configurator confirms that you want to delete the account before doing so.

41.3 ISP Account Edit

The **ISP Account Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See Section 41.2 on page 563.) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 411 Object > ISP Account > Edit



Configuration

Profile Name: Acc_1
Protocol: pppoe
Authentication Type: Chap/PAP
User Name: username
Password: ****
Retype to confirm: ****
Service Name: (optional)
Compression: ○ On ● Off
Idle timeout: 0 (Seconds)

The following table describes the labels in this screen.

Table 192 Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: **pppoe** - This ISP account uses the PPPoE protocol. **pptp** - This ISP account uses the PPTP protocol.

Table 192 Object > ISP Account > Edit (continued)

LABEL	**DESCRIPTION**
Encryption Method	This field is available if this ISP account uses the **PPTP** protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **nomppe** - This ISP account does not use MPPE. **mppe-40** - This ISP account uses 40-bit MPPE. **mppe-128** - This ISP account uses 128-bit MMPE.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accepts PAP only. **MSCHAP** - Your ZyWALL accepts MSCHAP only. **MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Server IP	If this ISP account uses the PPPoE protocol, this field is not displayed. If this ISP account uses the PPTP protocol, type the IP address of the PPTP server.
Connection ID	This field is available if this ISP account uses the **PPTP** protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select **On** button to turn on stac compression, and select **Off** to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the ZyWALL automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click **OK** to save your changes back to the ZyWALL. If there are no errors, the program returns to the **ISP Account** screen. If there are errors, a message box explains the error, and the program stays in the **ISP Account Edit** screen.
Cancel	Click **Cancel** to return to the **ISP Account** screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

42

SSL Application

This chapter describes how to configure SSL application objects for use in SSL VPN.

42.1 SSL Application Overview

Configure an SSL application object to specify a service and a corresponding IP address of the server on the local network. You can apply one or more SSL application objects in the **VPN > SSL VPN** screen for a user account/user group.

42.1.1 Application Types

The following lists the types of SSL applications you can configure on the ZyWALL.

- Web-based

  A web-based application allows remote users to access an intranet site using standard web browsers.
- File sharing

  Configure file sharing to allow users to access files on the intranet.

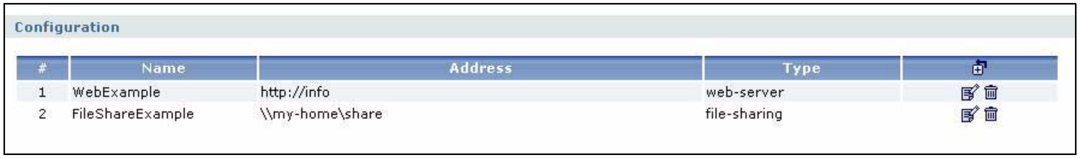
42.1.2 Remote User Screen Links

Available SSL application names are displayed as links in remote user screens. Depending on the application type, remote users can simply click the links or follow the steps in the pop-up dialog box to access.

42.2 SSL Application Configuration

The main **SSL Application** screen displays a list of the configured SSL application objects. Click **Object > SSL Application** in the navigation panel.

Figure 412 Object > SSL Application



Configuration

#	Name	Address	Type
1	WebExample	http://info	web-server
2	FileShareExample	\\my-home\share	file-sharing

The following table describes the labels in this screen.

Table 193 Object > SSL Application

LABEL	DESCRIPTION
#	This field displays the index number.
Name	This field displays the name of the object.
Address	This field displays the IP address/URL of the application server or the location of a file share.
Type	This field display the application type.
Add icon	This column provides icons to add, edit, and remove SSL application objects. To add an object, click the **Add** icon at the top of the column. To edit an object, click the **Edit** icon next to the object. To delete an object, click the **Remove** icon next to the object.

42.3 Creating/Editing an SSL Application

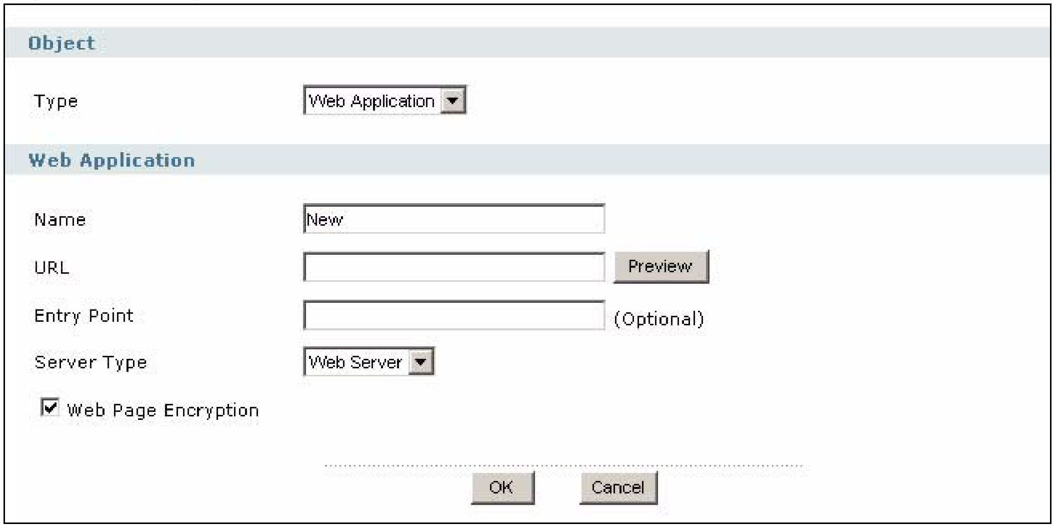
To create or edit an SSL application object, click the **Add** or **Edit** button in the **SSL Application** screen. There are two types of SSL applications: web-based and file sharing.

42.3.1 Web-based Application

A web-based application allows remote users to access an application via standard web browsers.

To configure a web-based application, click the **Add** or **Edit** button in the **SSL Application** screen and select **Web Application** in the **Type** field to display the configuration screen as shown.

Figure 413 Object > SSL Application > Add/Edit: Web Application



Object

Type: Web Application

Web Application

Name: New

URL:

Entry Point: (Optional)

Server Type: Web Server

☑ Web Page Encryption

The following table describes the labels in this screen.

Table 194 Object > SSL Application > Add/Edit: Web Application

LABEL	DESCRIPTION
Object	
Type	Select **Web Application** from the drop-down list box.
Web Application	
Name	Enter a descriptive name to identify this object. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). No spaces are allowed. Note: If there is any space in the name, a warning screen displays when you click Apply. The ZyWALL will also automatically delete the space(s).
URL	Enter the fully qualified domain name (FQDN) or IP address of the application server. Note: You must enter the “http://” or “https://” prefix. Remote users are restricted to access only files in this directory. For example, if you enter “\remote\” in this field, emote users can only access files in the “remote” directory. If a link contains a file that is not within this domain, then remote users cannot access it.
Preview	Click **Preview** to access the URL you specified in a new IE web browser.
Entry Point	This field is optional. You only need to configure this field if you need to specify the name of the directory or file on the local server as the home page or home directory on the user screen.
Server Type	Specify the type of service for this SSL application. Select **Web Server** to allow access to the specified web site hosted on the local network. Select **OWA** (Outlook Web Access) to allow users to access e-mails, contacts, calenders via Microsoft Outlook-like interface using supported web browsers. The ZyWALL supports one OWA object.
Web Page Encryption	Select this option to prevent users from saving the web content.
Ok	Click **Ok** to save the changes and return to the main **SSL Application Configuration** screen.
Cancel	Click **Cancel** to discard the changes and return to the main **SSL Application Configuration** screen.

42.3.2 Example: Specifying a Web Site for Access

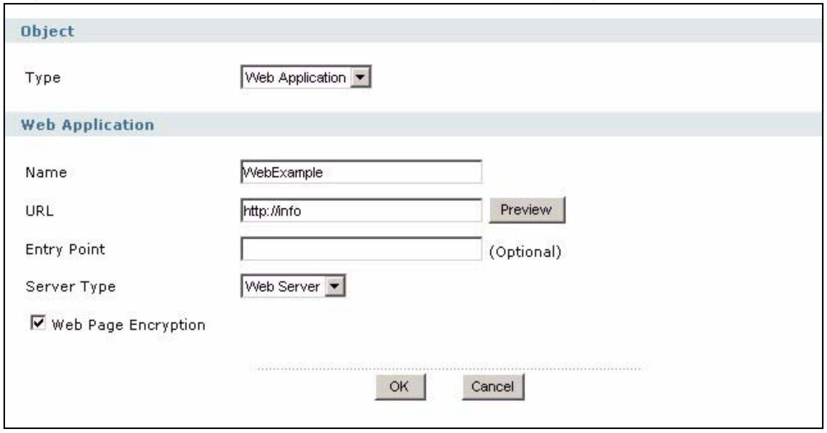
This example shows you how to create a web-based application for an internal web site. The address of the web site is http://info with web page encryption.

1. Click **Object** > **SSL Application** in the navigation panel.
2. Click the **Add** button and select **Web Application** in the **Type** field.
3. Enter a descriptive name in the **Display Name** field. For example, “CompanyIntranet”.
4. In the **Address** field, enter “http://info”.
5. In the **Server Type** field, select **Web Server**.
6. Select **Web Page Encryption** to prevent users from saving the web content.

7 Click **Apply** to save the settings.

The configuration screen should look similar to the following figure.

Figure 414 Example: SSL Application: Specifying a Web Site for Access



Object

Type: Web Application

Web Application

Name: WebExample

URL: http://info

Entry Point: (Optional)

Server Type: Web Server

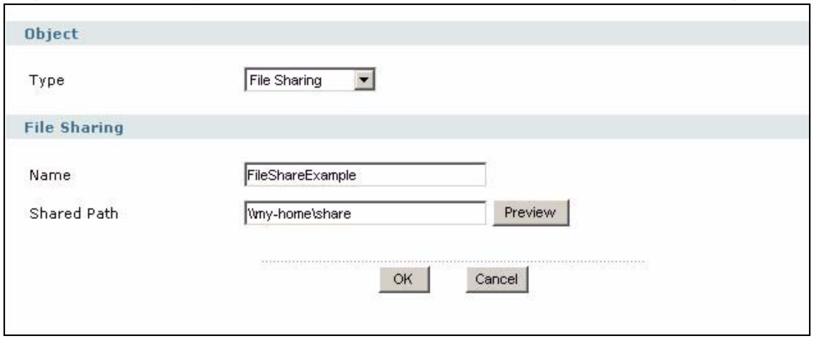
☑ Web Page Encryption

42.3.3 Configuring File Sharing

You can specify the name of a folder on a file server (Linux or Windows) which remote users can access. Remote users can access files using a standard web browser and files are displayed as links on the screen.

To configure a file share, click the **Add** or **Edit** button in the **SSL Application** screen and select **File Sharing** in the **Type** field. The configuration screen displays as shown.

Figure 415 Object > SSL Application > Add/Edit: File Sharing



Object

Type: File Sharing

File Sharing

Name: FileShareExample

Shared Path: \\my-home\share

The following table describes the labels in this screen.

Table 195 Object > SSL Application > Add/Edit: Web Application

LABEL	DESCRIPTION
Object	
Type	Select File Sharing to create a file share application for VPN SSL.
File Sharing	
Name	Enter a descriptive name to identify this object. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”).

Table 195 Object > SSL Application > Add/Edit: Web Application

LABEL	DESCRIPTION
Shared Path	Specify the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats. "\\<IP address>\<share name>" "\\<domain name>\<share name>" "\\<computer name>\<share name>" For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer.
Preview	Click **Preview** to display the file share in a new web browser.
Ok	Click **Ok** to save the changes and return to the main **SSL Application Configuration** screen.
Cancel	Click **Cancel** to discard the changes and return to the main **SSL Application Configuration** screen.

You must then configure the shared folder on the file server for remote access. Refer to the document that comes with your file server.

PART VI

System

System (575)
Service Control (587)

43

System

This chapter provides information on the general system screens. See Chapter 44 on page 587 for details on the system screens that control service access.

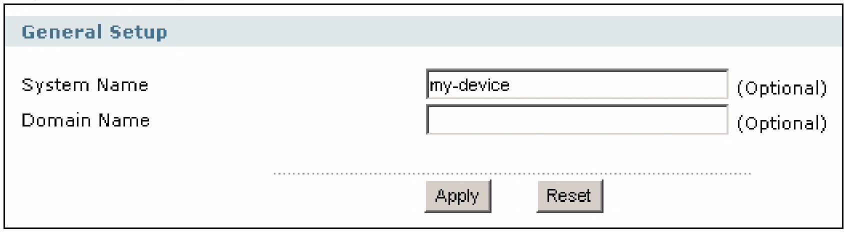
43.1 System Overview

The system screens can help you configure general ZyWALL information, the system time and the console port connection speed for a terminal emulation program. The screens also allow you to configure DNS settings and determine which services/protocols can access which ZyWALL zones (if any) from which computers.

43.2 Host Name

A host name is the unique name by which a device is known on a network. Click **System > Host Name** to open the **Host Name** screen.

Figure 416 System > Host Name



System Name: my-device (Optional)

Domain Name: (Optional)

The following table describes the labels in this screen.

Table 196 System > Host Name

LABEL	DESCRIPTION
General Settings	
System Name	Choose a descriptive name to identify your ZyWALL device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes “-” are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes “-” are accepted.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

43.3 Time and Date

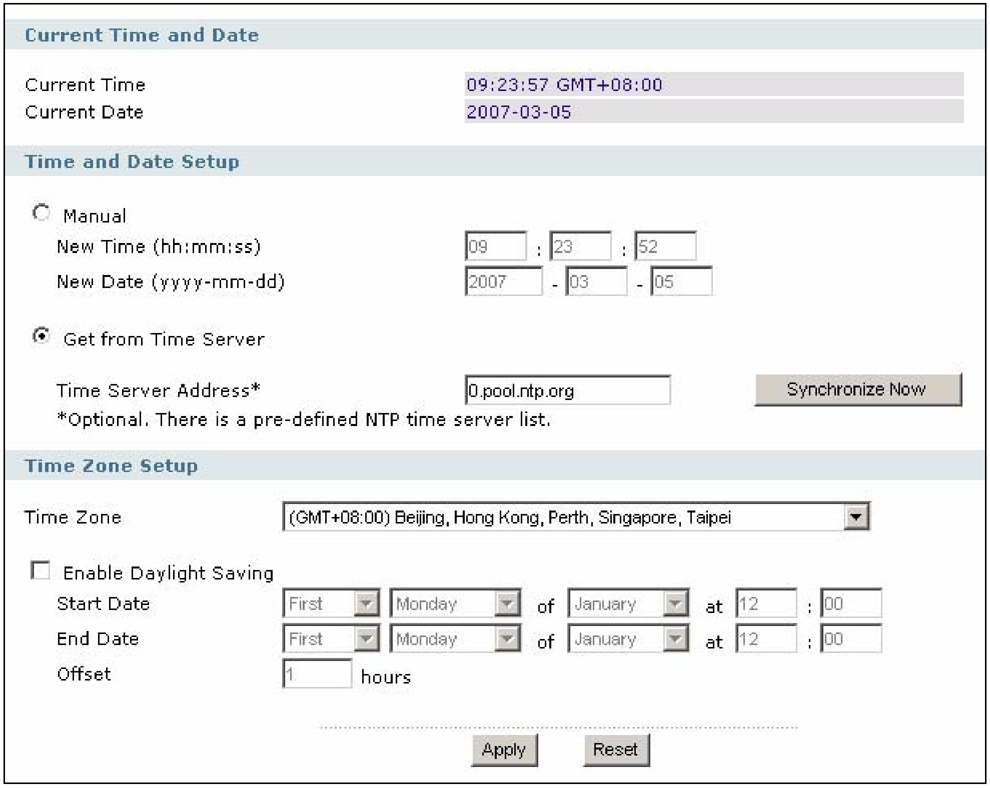
This section shows you how:

1. To manually set the ZyWALL date and time.
2. To get the ZyWALL date and time from a time server.

For effective scheduling and logging, the ZyWALL system time must be accurate. The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your ZyWALL's time based on your local time zone and date, click **System > Date/Time**. The screen displays as shown.

Figure 417 System > Date and Time



Current Time and Date

Current Time: 09:23:57 GMT+08:00
Current Date: 2007-03-05

Time and Date Setup

○ Manual
New Time (hh:mm:ss): 09 : 23 : 52
New Date (yyyy-mm-dd): 2007 - 03 - 05

● Get from Time Server
Time Server Address*: 0.pool.ntp.org
*Optional. There is a pre-defined NTP time server list.

Time Zone Setup

Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

☐ Enable Daylight Saving
Start Date: First Monday of January at 12 : 00
End Date: First Monday of January at 12 : 00
Offset: 1 hours

The following table describes the labels in this screen.

Table 197 System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your ZyWALL.
Current Date	This field displays the present date of your ZyWALL.
Time and Date Setup	

Table 197 System > Date and Time (continued)

LABEL	DESCRIPTION
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the ZyWALL uses the new setting once you click **Apply**.
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyWALL get the time and date from the time server you specify below. The ZyWALL requests time and date settings from the time server under the following circumstances. • When the ZyWALL starts up. • When you click **Apply** or **Synchronize Now** in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the ZyWALL get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 197 System > Date and Time (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

43.3.1 Pre-defined NTP Time Servers List

When you turn on the ZyWALL for the first time, the date and time start at 2003-01-01 00:00:00. The ZyWALL then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The ZyWALL continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 198 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

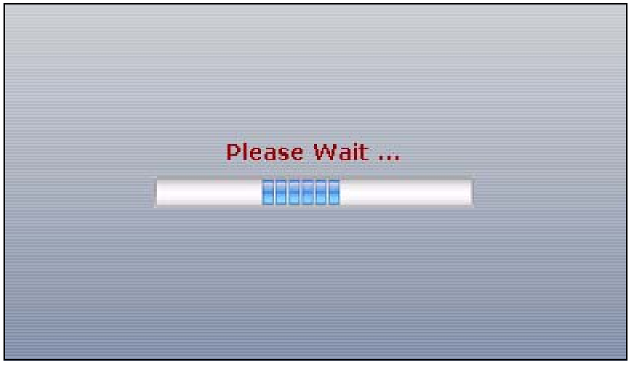
When the ZyWALL uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

43.3.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Please Wait...** screen appears, you may have to wait up to one minute.

Figure 418 Synchronization in Process



Please Wait ...

The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try reconfiguring the **Date/Time** screen.

To manually set the ZyWALL date and time.

1. Click **System** > **Date/Time**.
2. Select **Manual** under **Time and Date Setup**.
3. Enter the ZyWALL's time in the **New Time** field.
4. Enter the ZyWALL's date in the **New Date** field.
5. Under **Time Zone Setup**, select your **Time Zone** from the list.
6. As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.
7. Click **Apply**.

To get the ZyWALL date and time from a time server

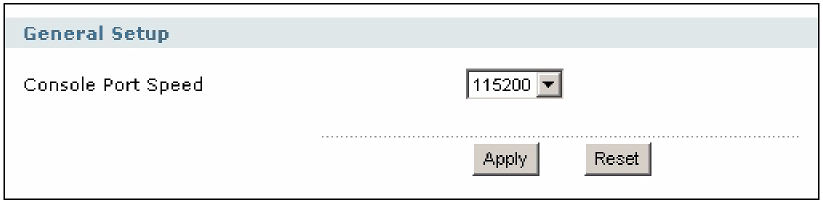
1. Click **System** > **Date/Time**.
2. Select **Get from Time Server** under **Time and Date Setup**.
3. Under **Time Zone Setup**, select your **Time Zone** from the list.
4. As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.
5. Under **Time and Date Setup**, enter a **Time Server Address** (Table 198 on page 578).
6. Click **Apply**.

43.4 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program. See Table 2 on page 55 for default console port settings.

Click **System** > **Console Speed** to open the **Console Speed** screen.

Figure 419 System > Console Port Speed



The following table describes the labels in this screen.

Table 199 System > Console Port Speed

LABEL	DESCRIPTION
Configuration	
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your ZyWALL supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The **Console Port Speed** applies to a console port connection using terminal emulation software and NOT the **Console** in the ZyWALL web configurator **Status** screen.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

43.5 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

43.5.1 DNS Server Address Assignment

The ZyWALL can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

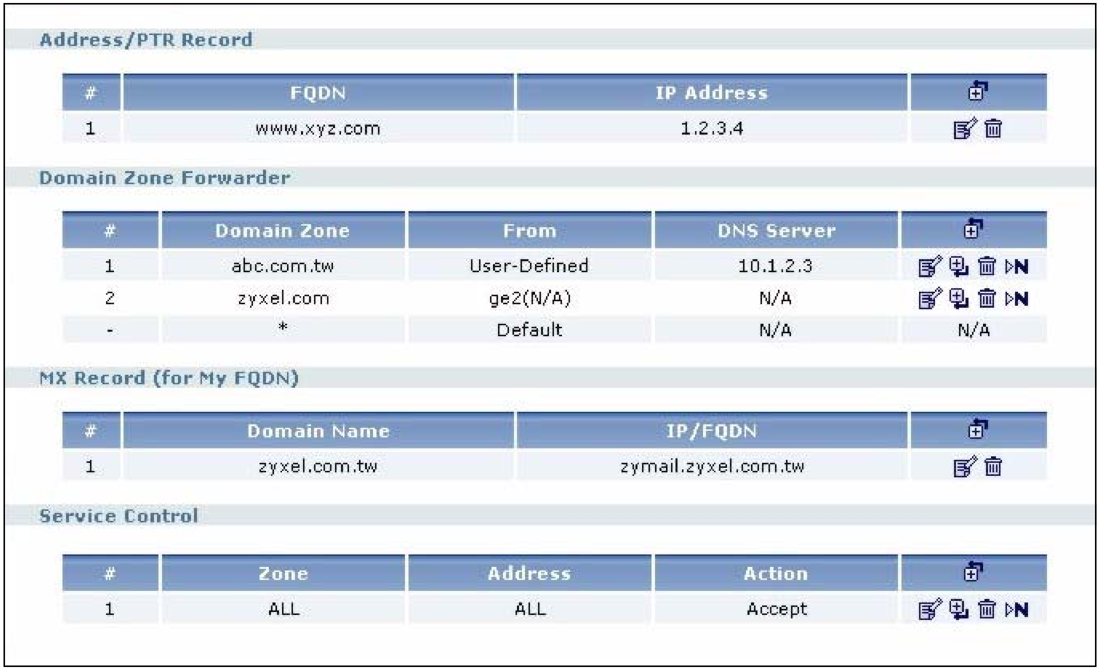
43.5.2 DNS Servers

Use the **DNS** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server. You can also configure the ZyWALL to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the ZyWALL sends to the specified DHCP client devices.

43.5.3 Configuring DNS

Click **System > DNS** to change your ZyWALL's DNS settings.

Figure 420 System > DNS



Address/PTR Record

#	FQDN	IP Address	
1	www.xyz.com	1.2.3.4	

Domain Zone Forwarder

#	Domain Zone	From	DNS Server	
1	abc.com.tw	User-Defined	10.1.2.3	
2	zyxel.com	ge2(N/A)	N/A	
-	*	Default	N/A	N/A

MX Record (for My FQDN)

#	Domain Name	IP/FQDN	
1	zyxel.com.tw	zymail.zyxel.com.tw	

Service Control

#	Zone	Address	Action	
1	ALL	ALL	Accept	

The following table describes the labels in this screen.

Table 200 System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
#	This is the index number of the address/PTR record.
FQDN	This is a host’s fully qualified domain name.
IP Address	This is the IP address of a host.
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new address/PTR record. Refer to Table 201 on page 583 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the record. Click the **Delete** icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Domain Zone Forwarder	This specifies a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the ZyWALL needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A “*” means all domain zones. The default record is not configurable. The ZyWALL uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.

Table 200 System > DNS (continued)

LABEL	DESCRIPTION
From	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually.
DNS Server	This is the IP address of a DNS server. This field displays **N/A** if you have the ZyWALL get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new domain zone forwarder record. Refer to Table 202 on page 584 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the record. Click the **Add** icon in an entry to add a record below the current entry. Click the **Delete** icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that record and press [ENTER] to move the record to the number that you typed.
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or fully qualified domain name of a mail server that handles the mail for the domain specified in the field above.
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new MX record. Refer to Table 203 on page 585 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the record. Click the **Delete** icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Service Control	This specifies from which computers and zones you can send DNS queries to the ZyWALL.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the ZyWALL accepts DNS queries from the computer with the IP address specified above through the specified zone (**Accept**) or discards them (**Deny**).
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 204 on page 586 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.

43.5.4 Address Record

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com” is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where “mail” is the host, “myZyXEL” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.

The ZyWALL allows you to configure address records about the ZyWALL itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server.

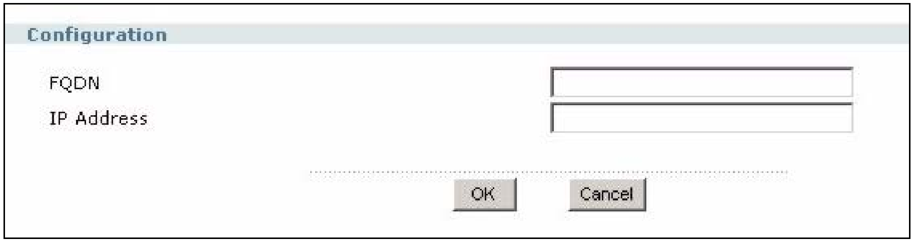
43.5.5 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

43.5.6 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an address/PTR record.

Figure 421 System > DNS > Address/PTR Record Edit



The following table describes the labels in this screen.

Table 201 System > DNS > Address/PTR Record Edit

LABEL	DESCRIPTION
FQDN	Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed.
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

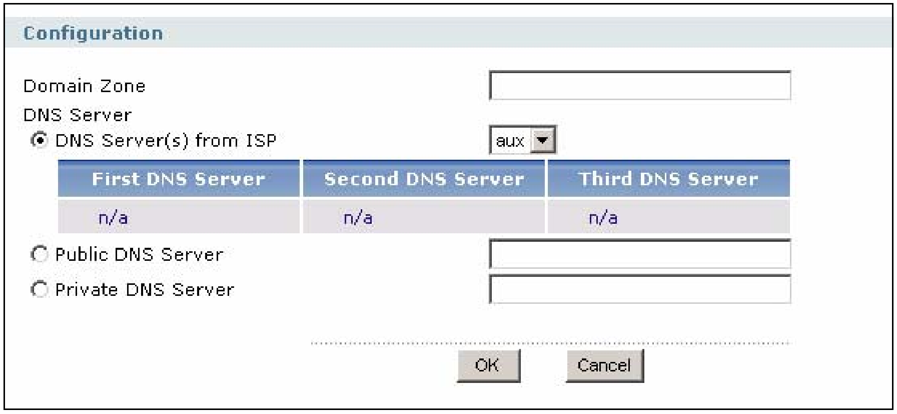
43.5.7 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

43.5.8 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a **domain zone forwarder** record.

Figure 422 System > DNS > Domain Zone Forwarder Edit



The following table describes the labels in this screen.

Table 202 System > DNS > Domain Zone Forwarder Edit

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select **DNS Server(s) from ISP** if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select **Public DNS Server** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The ZyWALL must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the ZyWALL's local networks. You cannot use 0.0.0.0. Select **Private DNS Server** if you have the IP address of a DNS server to which the ZyWALL connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

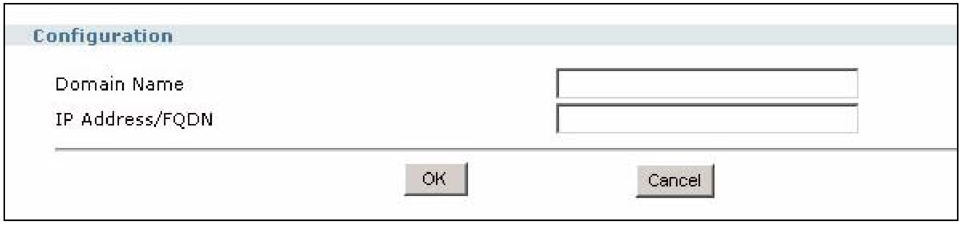
43.5.9 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

43.5.10 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

Figure 423 System > DNS > MX Record Edit



The following table describes the labels in this screen.

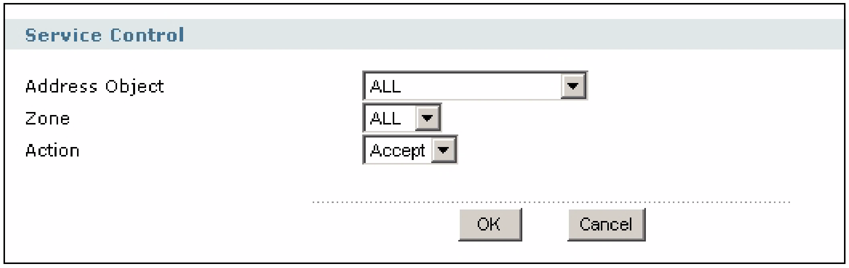
Table 203 System > DNS > MX Record Edit

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or fully qualified domain name of a mail server that handles the mail for the domain specified in the field above.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

43.5.11 DNS Service Control

Click the **Add** icon in the **Service Control** table to add a service control rule.

Figure 424 System > DNS > Service Control Rule Edit



Address Object: ALL
Zone: ALL
Action: Accept

The following table describes the labels in this screen.

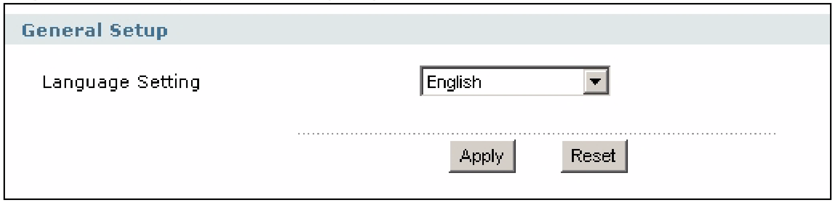
Table 204 System > DNS > Service Control Rule Edit

LABEL	DESCRIPTION
Address Object	Select **ALL** to allow or deny any computer to send DNS queries to the ZyWALL. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the ZyWALL.
Zone	Select **ALL** to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the ZyWALL is allowed or denied.
Action	Select **Accept** to have the ZyWALL allow the DNS queries from the specified computer. Select **Deny** to have the ZyWALL reject the DNS queries from the specified computer.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

43.6 Language Screen

Click **System > Language** to open the following screen. Use this screen to select a display language for the ZyWALL's web configurator screens.

Figure 425 System > Language



General Setup

Language Setting: English

The following table describes the labels in this screen.

Table 205 System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the ZyWALL's web configurator screens. You also need to open a new browser session to display the screens in the new language.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44

Service Control

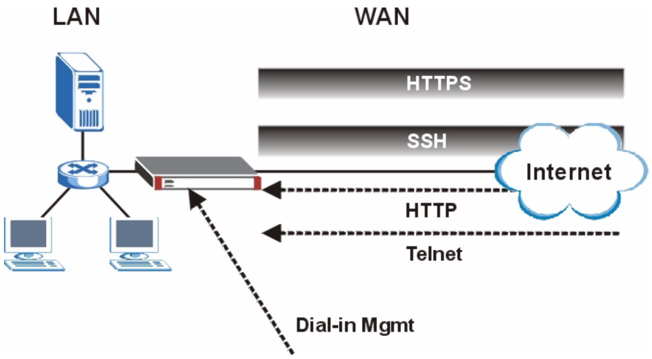
This chapter covers controlling access to the ZyWALL. See Chapter 43 on page 575 for the general system configuration screens.

44.1 Service Control Overview

Use this chapter to control which services can access the ZyWALL.

The following figure shows secure and insecure management of the ZyWALL coming in from the WAN. HTTPS and SSH access are secure. HTTP, Telnet, and dial-in management access are not secure.

Figure 426 Secure and Insecure Service Access From the WAN



See Section 5.6.1 on page 123 for related information on these screens.

To allow the ZyWALL to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ZyWALL firewall rule to block that traffic.

See Section 19.2.1.2 on page 279 for more on To-ZyWALL firewall rules.

To stop a service from accessing the ZyWALL, clear **Enable** in the corresponding service screen.

44.1.1 Service Access Limitations

A service cannot be used to access the ZyWALL when:

1. You have disabled that service in the corresponding screen.
2. The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the ZyWALL disallows the session).
3. The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
4. There is a firewall rule that blocks it.

44.1.2 System Timeout

There is a lease timeout for administrators. The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ZyWALL for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User/Group** screens.

44.2 HTTPS

You can set the ZyWALL to use HTTP or HTTPS (HTTPS adds security) for web configurator sessions. Specify which zones allow web configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

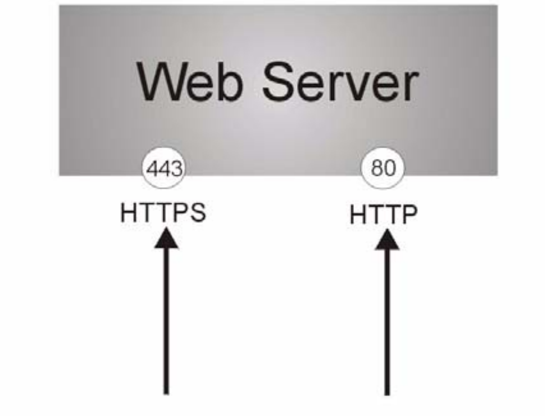
It relies upon certificates, public keys, and private keys (see Chapter 40 on page 545 for more information).

HTTPS on the ZyWALL is used so that you can securely access the ZyWALL using the web configurator. The SSL protocol specifies that the HTTPS server (the ZyWALL) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the ZyWALL), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the ZyWALL a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyWALL.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL's web server.
2. HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's web server.

Figure 427 HTTP/HTTPS Implementation



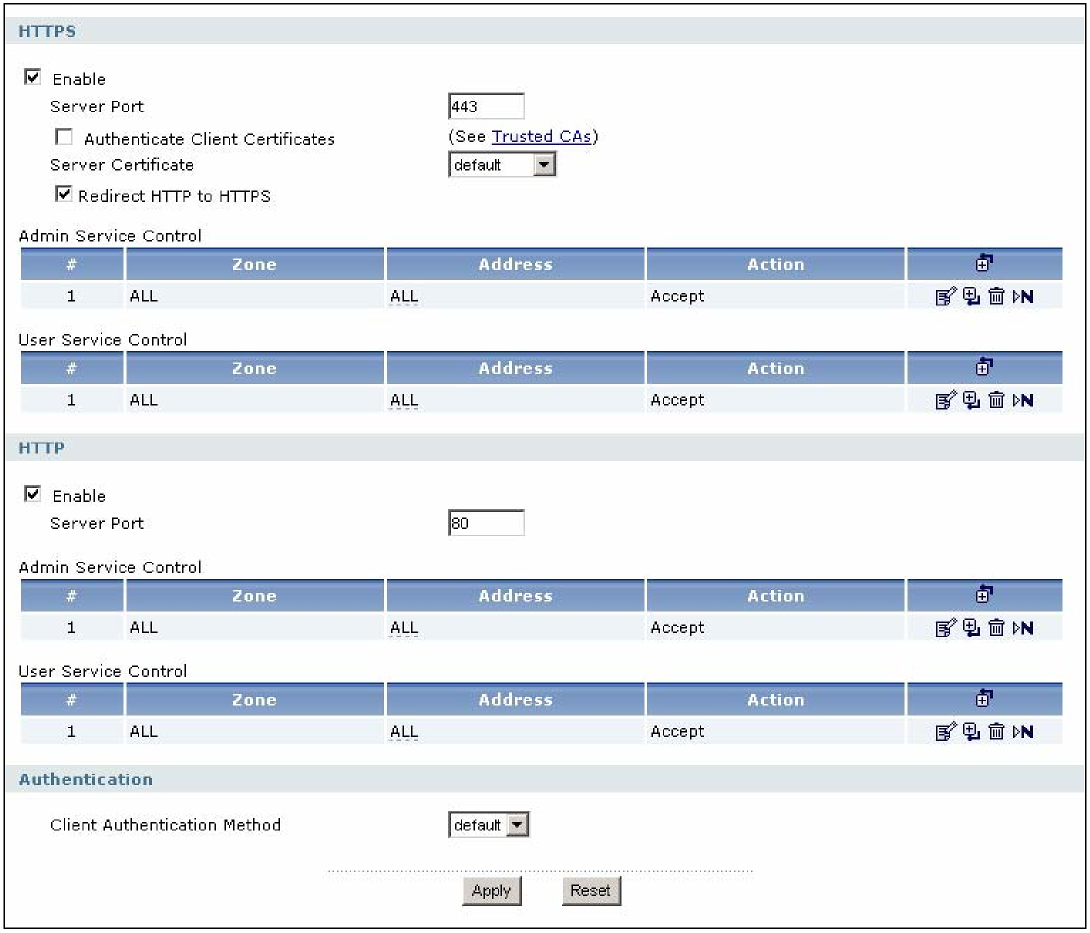
If you disable **HTTP** in the **WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

44.3 Configuring WWW

Click **System > WWW** to open the **WWW** screen. Use this screen to specify from which zones you can access the ZyWALL using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Admin Service Control deals with management access (to the web configurator).
User Service Control deals with user access to the ZyWALL (logging into SSL VPN for example).

Figure 428 System > WWW



HTTPS

☑ Enable

Server Port 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate default

☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

User Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

HTTP

☑ Enable

Server Port 80

Admin Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

User Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

Authentication

Client Authentication Method default

The following table describes the labels in this screen.

Table 206 System > WWW

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL web configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL web configurator to use “https://ZyWALL IP Address:**8443**” as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Section 44.5.5 on page 595 on importing certificates for details).
Server Certificate	Select a certificate the HTTPS server (the ZyWALL) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure web configurator access, select this to redirect all HTTP connection requests to the HTTPS server.

Table 206 System > WWW (continued)

LABEL	DESCRIPTION
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTPS to manage the ZyWALL (using the web configurator). You can also specify the IP addresses from which the administrators can manage the ZyWALL. **User Service Control** specifies from which zones a user can use HTTPS to log into the ZyWALL (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the ZyWALL.
#	This is the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 207 on page 592 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL web configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the ZyWALL.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTP to manage the ZyWALL (using the web configurator). You can also specify the IP addresses from which the administrators can manage the ZyWALL. **User Service Control** specifies from which zones a user can use HTTP to log into the ZyWALL (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the ZyWALL.
#	This is the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 207 on page 592 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Authentication	

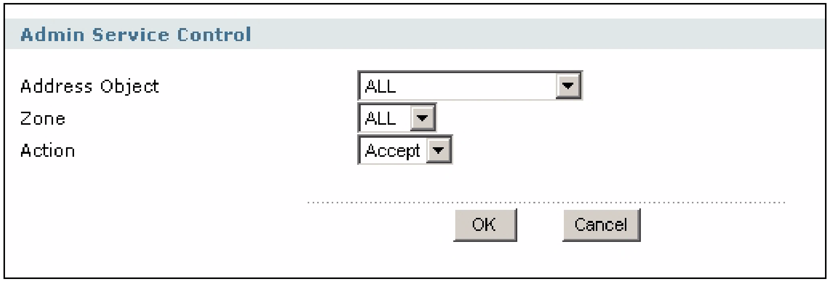
Table 206 System > WWW (continued)

LABEL	DESCRIPTION
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the **Auth. method** screen.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44.4 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW**, **SSH**, **Telnet**, **FTP** or **SNMP** screen to add a service control rule.

Figure 429 System > Service Control Rule Edit



Admin Service Control

Address Object: ALL

Zone: ALL

Action: Accept

The following table describes the labels in this screen.

Table 207 Edit Service Control Rule

LABEL	DESCRIPTION
Address Object	Select **ALL** to allow or deny any computer to communicate with the ZyWALL using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the ZyWALL using this service.
Zone	Select **ALL** to allow or prevent any ZyWALL zones from being accessed using this service. Select a predefined ZyWALL zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the ZyWALL from the specified computers. Select **Deny** to block the user's access to the ZyWALL from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

44.5 HTTPS Example

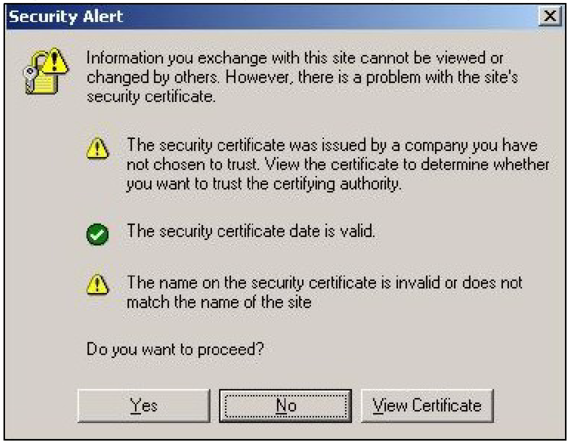
If you haven't changed the default HTTPS port on the ZyWALL, then in your browser enter "https://ZyWALL IP Address/" as the web site address where "ZyWALL IP Address" is the IP address or domain name of the ZyWALL you wish to access.

44.5.1 Internet Explorer Warning Messages

When you attempt to access the ZyWALL HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyWALL.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 430 Security Alert Dialog Box (Internet Explorer)



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

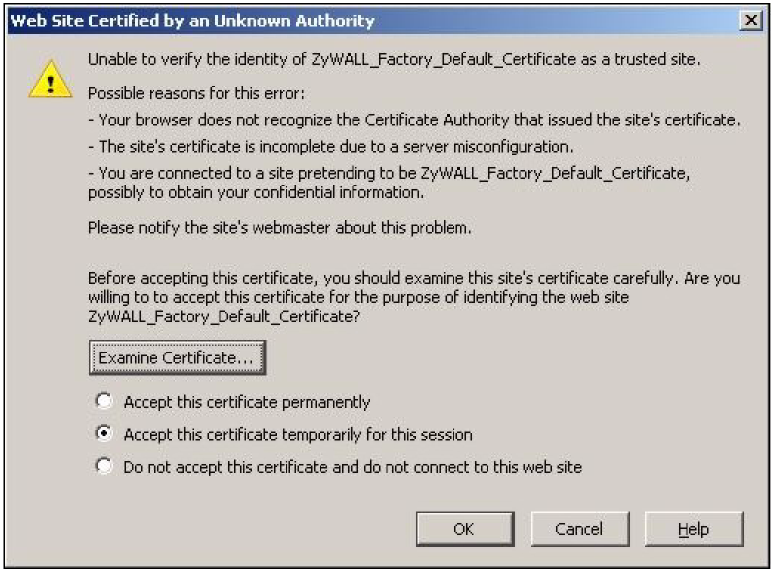
44.5.2 Netscape Navigator Warning Messages

When you attempt to access the ZyWALL HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyWALL.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyWALL's certificate into the SSL client.

Figure 431 Security Certificate 1 (Netscape)



Unable to verify the identity of ZyWALL_Factory_Default_Certificate as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL_Factory_Default_Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

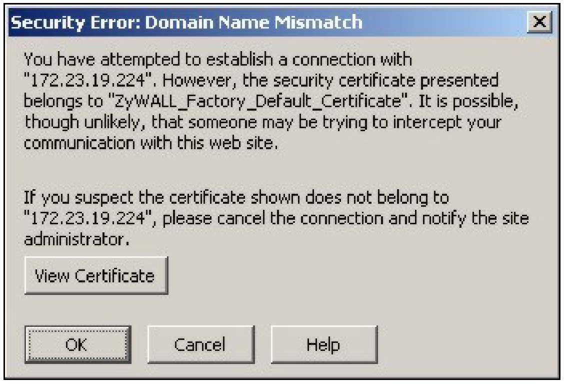
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site ZyWALL_Factory_Default_Certificate?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this web site

Figure 432 Security Certificate 2 (Netscape)



You have attempted to establish a connection with "172.23.19.224". However, the security certificate presented belongs to "ZyWALL_Factory_Default_Certificate". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "172.23.19.224", please cancel the connection and notify the site administrator.

44.5.3 Avoiding Browser Warning Messages

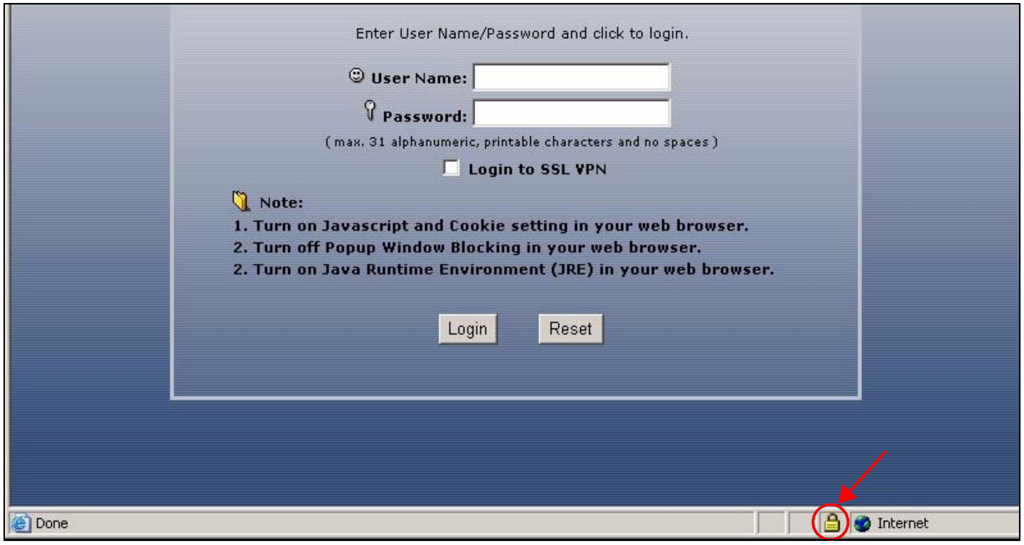
The following describes the main reasons that your browser displays warnings about the ZyWALL’s HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyWALL’s HTTPS server certificate is not one of the browser’s trusted certificate authorities. The issuing certificate authority of the ZyWALL's factory default certificate is the ZyWALL itself since the certificate is a self-signed certificate.
    - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
    - To have the browser trust the certificates issued by a certificate authority, import the certificate authority’s certificate into your operating system as a trusted certificate. Refer to Appendix E on page 713for details.

44.5.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 433 Login Screen (Internet Explorer)



Enter User Name/Password and click to login.

User Name:

Password:

(max. 31 alphanumeric, printable characters and no spaces)

☐ **Login to SSL VPN**

Note:

1. Turn on Javascript and Cookie setting in your web browser.

2. Turn off Popup Window Blocking in your web browser.

2. Turn on Java Runtime Environment (JRE) in your web browser.

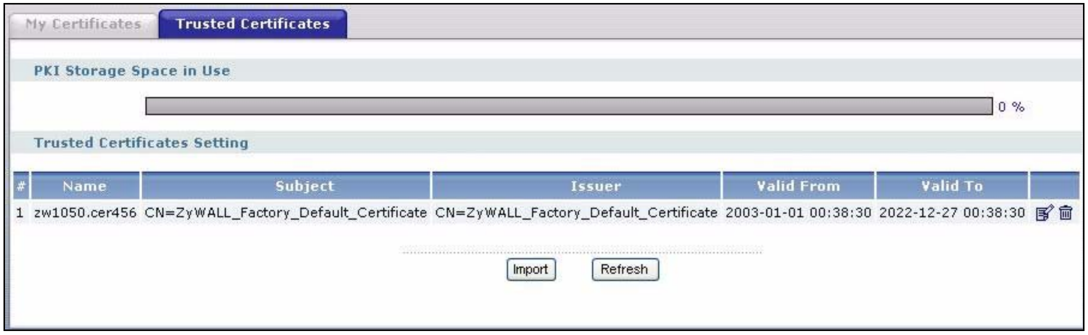
44.5.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL's **Trusted CA** web configurator screen).

Figure 434 ZyWALL Trusted CA Screen



PKI Storage Space in Use

0 %

Trusted Certificates Setting

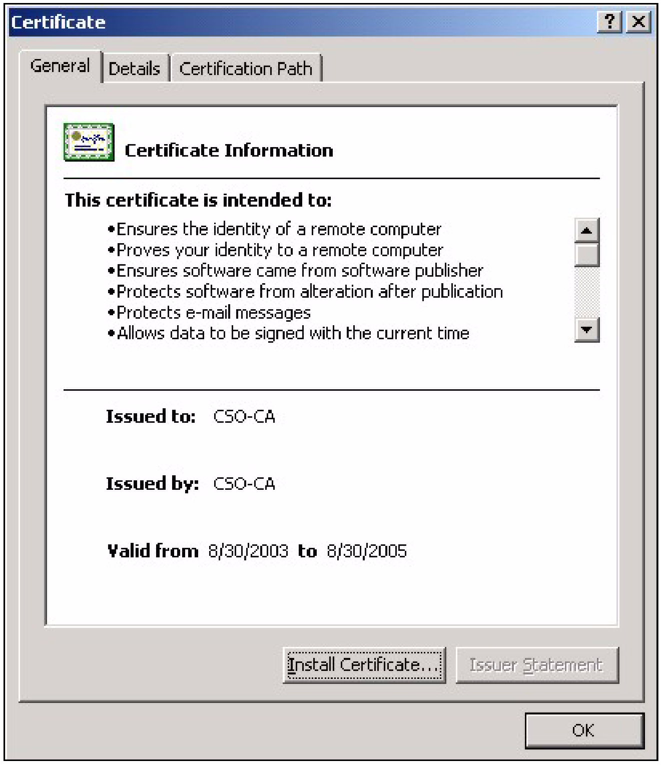
#	Name	Subject	Issuer	Valid From	Valid To	
1	zw1050.cer456	CN=ZyWALL_Factory_Default_Certificate	CN=ZyWALL_Factory_Default_Certificate	2003-01-01 00:38:30	2022-12-27 00:38:30	

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

44.5.5.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 435 CA Certificate Example



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: CSO-CA

Issued by: CSO-CA

Valid from 8/30/2003 **to** 8/30/2005

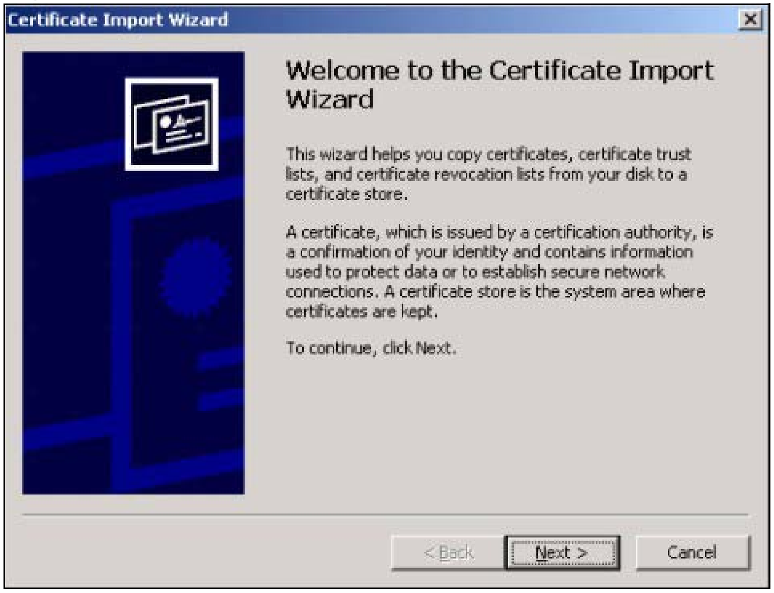
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

44.5.5.2 Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

Figure 436 Personal Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

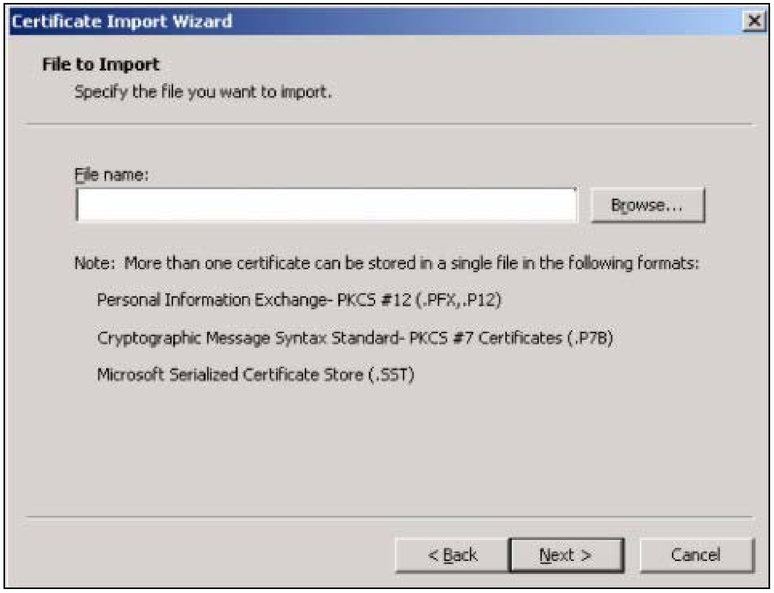
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 437 Personal Certificate Import Wizard 2



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

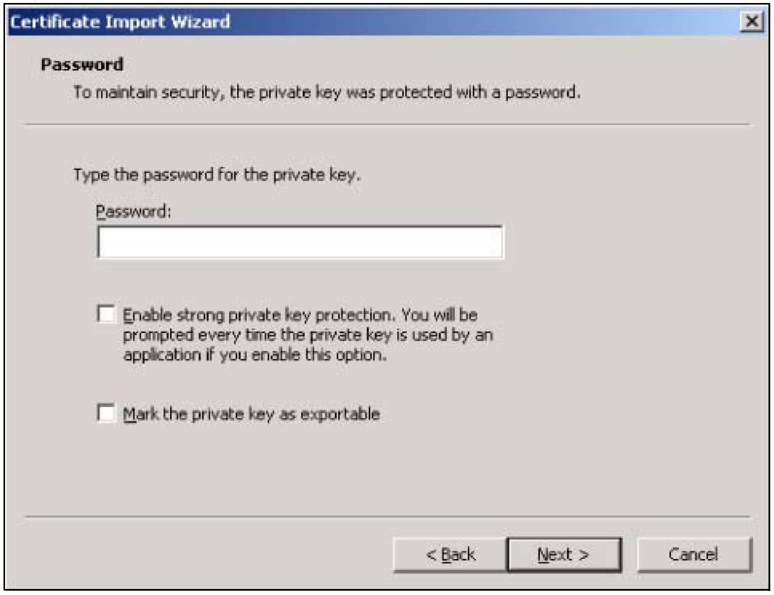
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

Figure 438 Personal Certificate Import Wizard 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

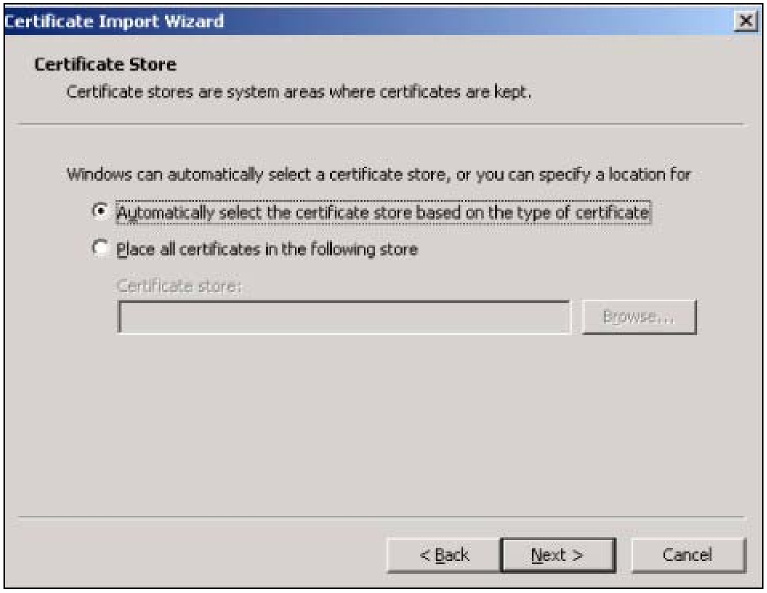
Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark the private key as exportable

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 439 Personal Certificate Import Wizard 4


Certificate Import Wizard
Certificate store:
Browse...
< Back
Next >
Cancel

Certificate Store

Certificate stores are system areas where certificates are kept.

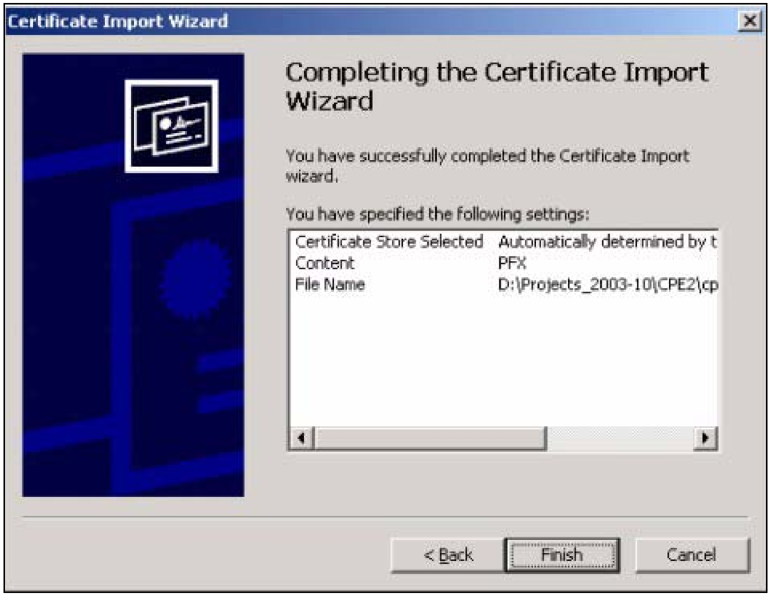
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

5 Click **Finish** to complete the wizard and begin the import process.

Figure 440 Personal Certificate Import Wizard 5


Certificate Import Wizard
< Back
Finish
Cancel

Completing the Certificate Import Wizard

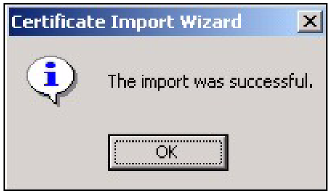
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	D:\Projects_2003-10\CPE2\cp

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 441 Personal Certificate Import Wizard 6


Certificate Import Wizard
OK

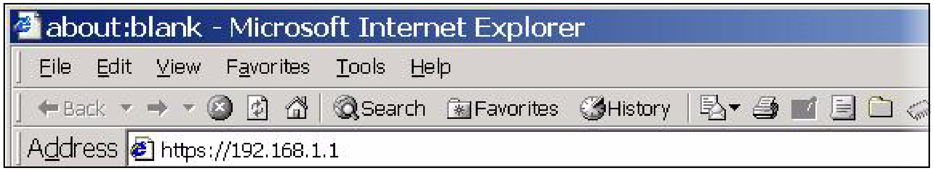
The import was successful.

44.5.6 Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

1 Enter 'https://ZyWALL IP Address/ in your browser's web address field.

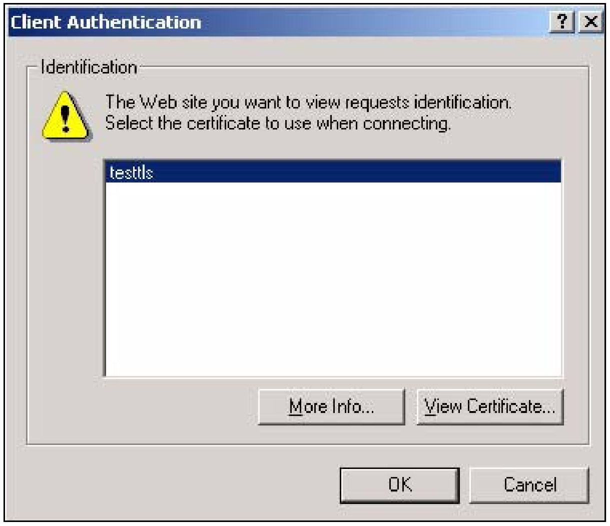
Figure 442 Access the ZyWALL Via HTTPS


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address

https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the ZyWALL, the following screen asks you to select a personal certificate to send to the ZyWALL. This screen displays even if you only have a single certificate as in the example.

Figure 443 SSL Client Authentication

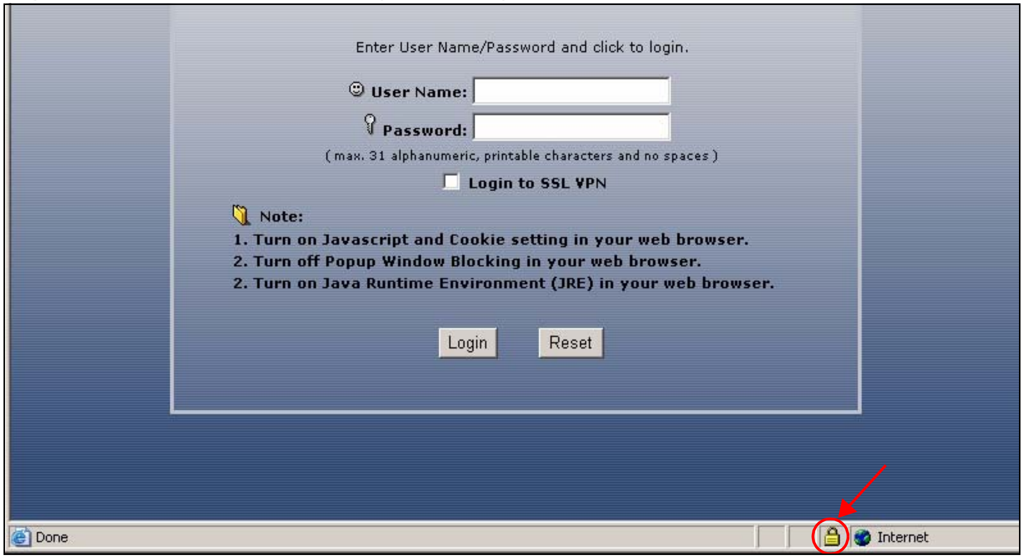

Client Authentication
Identification
More Info...
View Certificate...
OK
Cancel

The Web site you want to view requests identification. Select the certificate to use when connecting.

testtls

3 You next see the web configurator login screen.

Figure 444 Secure Web Configurator Login Screen


User Name:
Password:
☐ Login to SSL VPN
Login
Reset
Done
Internet

Enter User Name/Password and click to login.

(max. 31 alphanumeric, printable characters and no spaces)

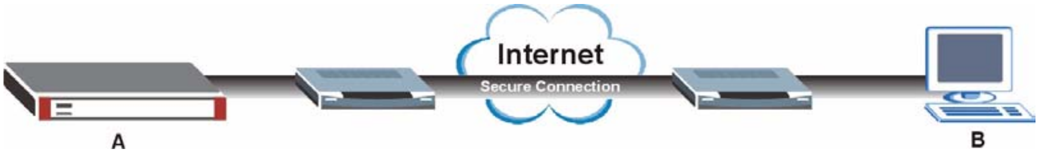
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
2. Turn on Java Runtime Environment (JRE) in your web browser.

44.6 SSH

You can use SSH (Secure SHell) to securely access the ZyWALL's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the ZyWALL for a management session.

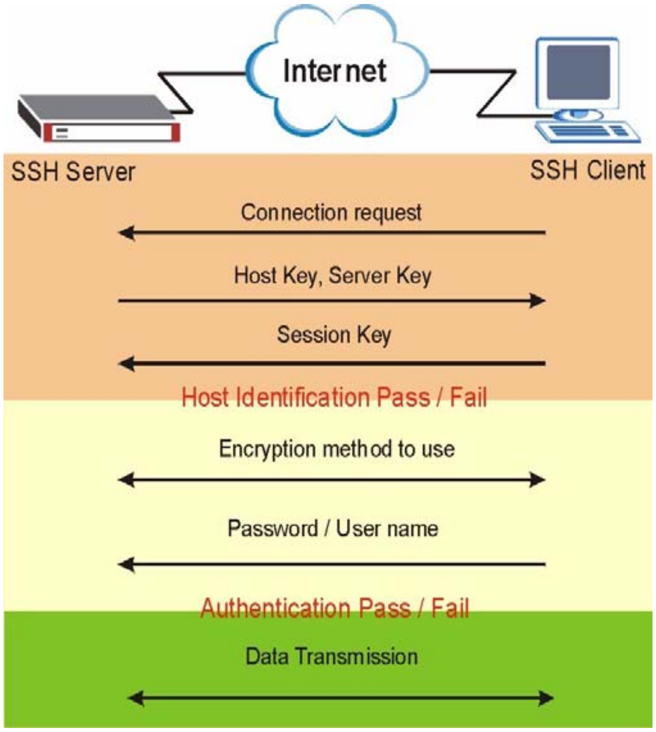
Figure 445 SSH Communication Over the WAN Example


Internet
Secure Connection
A
B

44.6.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 446 How SSH v1 Works Example


Internet
SSH Server
SSH Client
Connection request
Host Key, Server Key
Session Key
Host Identification Pass / Fail
Encryption method to use
Password / User name
Authentication Pass / Fail
Data Transmission

1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

44.6.2 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour and Blowfish). The SSH server is implemented on the ZyWALL for management using port 22 (by default).

44.6.3 Requirements for Using SSH

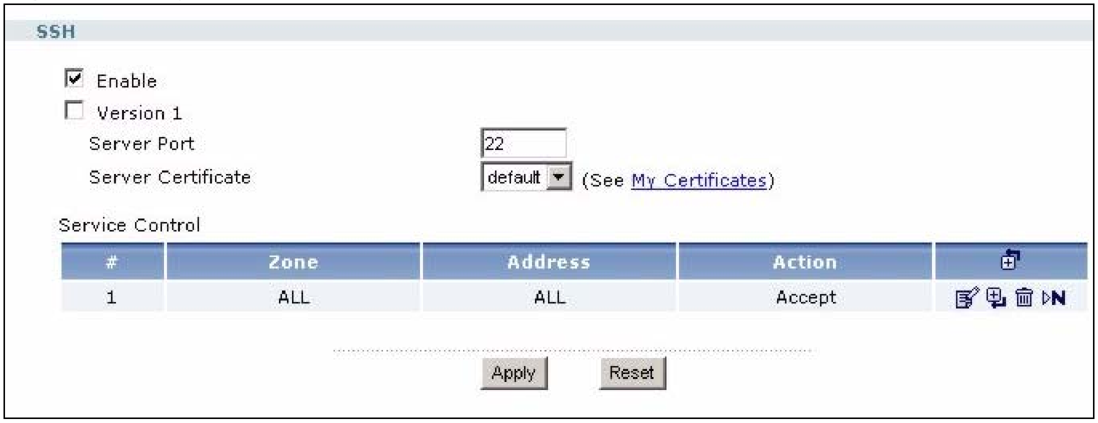
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

44.6.4 Configuring SSH

Click **System > SSH** to change your ZyWALL's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the ZyWALL. You can also specify from which IP addresses the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 447 System > SSH



SSH

☑ Enable

☐ Version 1

Server Port: 22

Server Certificate: default (See My Certificates)

Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

The following table describes the labels in this screen.

Table 208 System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL CLI using this service.
Version 1	Select the check box to have the ZyWALL use both SSH version 1 and version 2 protocols. If you clear the check box, the ZyWALL uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 40 on page 545 for details).
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 207 on page 592 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44.7 Secure Telnet Using SSH Examples

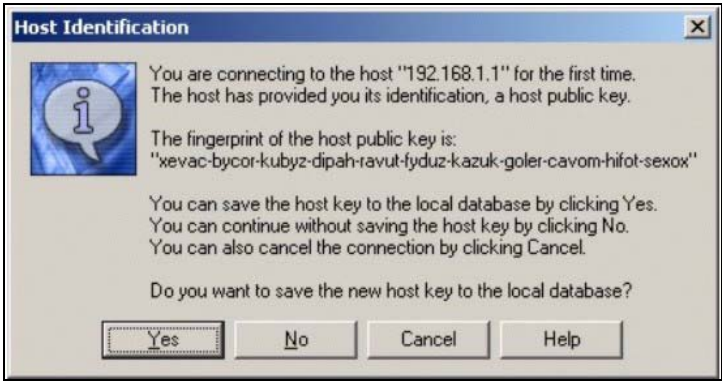
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyWALL. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

44.7.1 Example 1: Microsoft Windows

This section describes how to access the ZyWALL using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number) for the ZyWALL.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 448 SSH Example 1: Store Host Key



You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.

The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"

You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.

Do you want to save the new host key to the local database?

Enter the password to log in to the ZyWALL. The CLI screen displays next.

44.7.2 Example 2: Linux

This section describes how to access the ZyWALL using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the ZyWALL.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyWALL (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the ZyWALL.

Figure 449 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the ZyWALL using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "`yes`" and press [ENTER].

Then enter the password to log in to the ZyWALL.

Figure 450 SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI screen displays next.

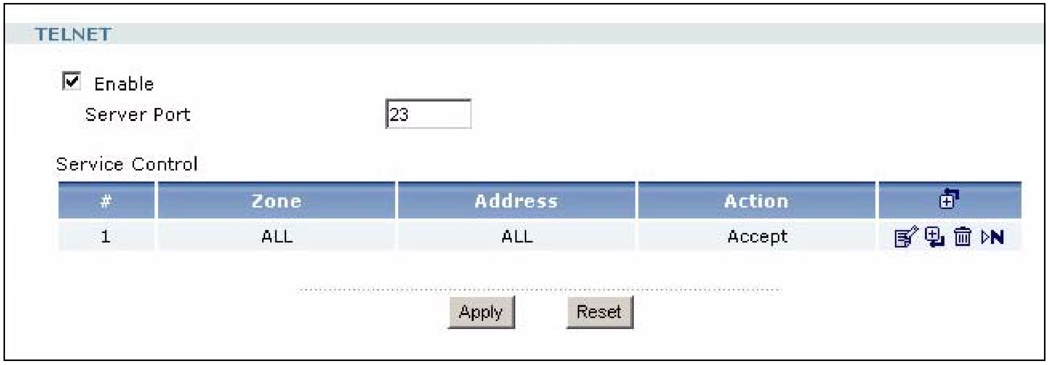
44.8 Telnet

You can use Telnet to access the ZyWALL's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

44.8.1 Configuring Telnet

Click **System > TELNET** to configure your ZyWALL for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 451 System > Telnet



The following table describes the labels in this screen.

Table 209 System > Telnet

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 207 on page 592 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.

Table 209 System > Telnet (continued)

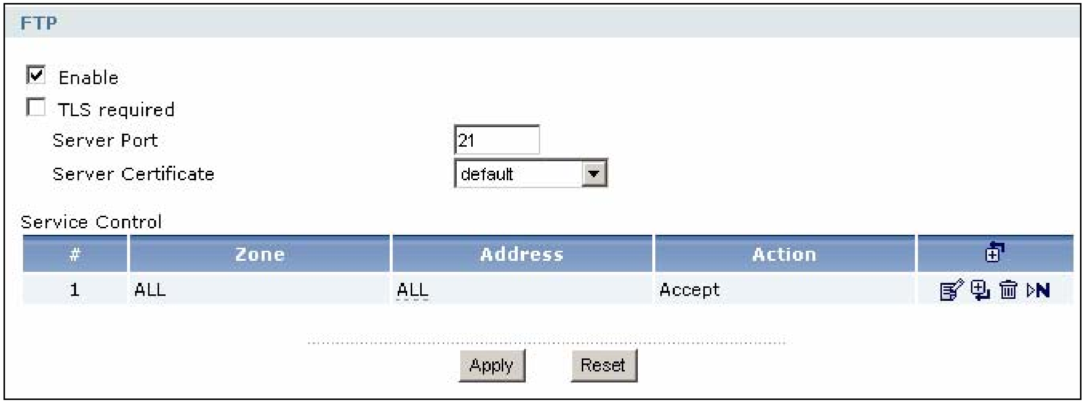
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44.9 Configuring FTP

You can upload and download the ZyWALL’s firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. Please see Chapter 45 on page 615 for more information about firmware and configuration files.

To change your ZyWALL’s FTP settings, click **System > FTP** tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 452 System > FTP



FTP

☑ Enable

☐ TLS required

Server Port: 21

Server Certificate: default

Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

The following table describes the labels in this screen.

Table 210 System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for FTP connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 40 on page 545 for details).
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.

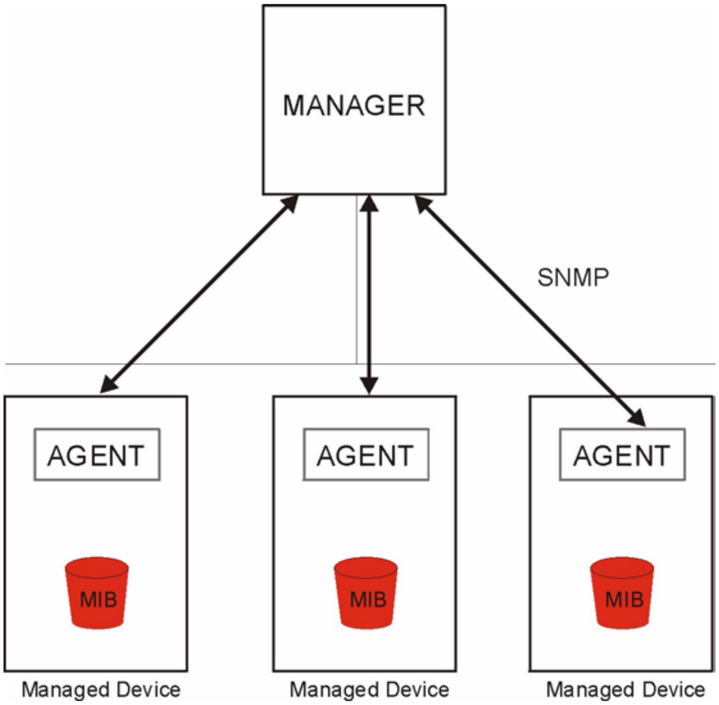
Table 210 System > FTP (continued)

LABEL	DESCRIPTION
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 207 on page 592 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44.10 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 453 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

44.10.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the ZyWALL's MIBs from www.zyxel.com.

44.10.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs.

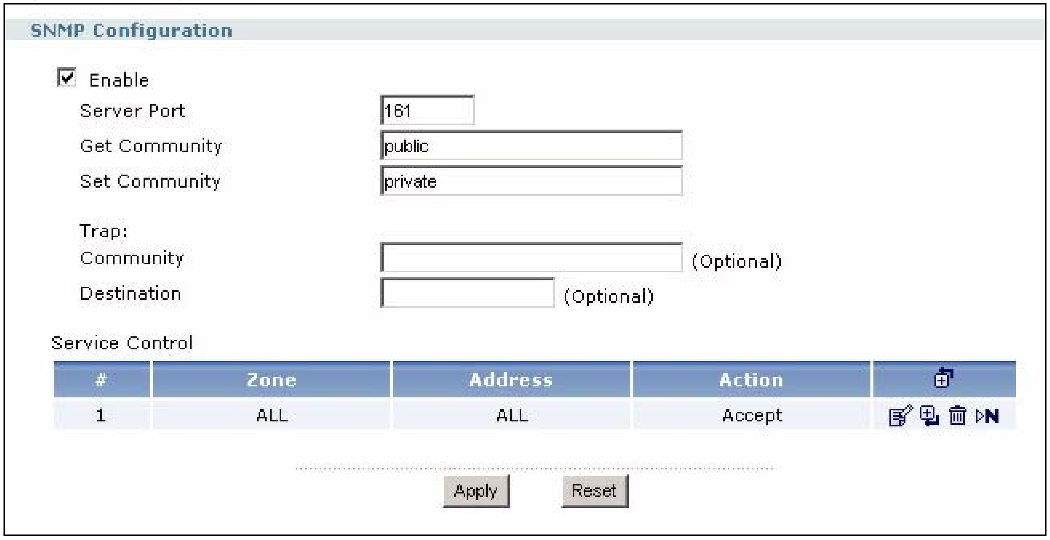
Table 211 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ZyWALL is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

44.10.3 Configuring SNMP

To change your ZyWALL's SNMP settings, click **System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 454 System > SNMP



SNMP Configuration

☑ Enable

Server Port: 161

Get Community: public

Set Community: private

Trap:

Community: (Optional)

Destination: (Optional)

Service Control

#	Zone	Address	Action
1	ALL	ALL	Accept

The following table describes the labels in this screen.

Table 212 System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).

Table 212 System > SNMP (continued)

LABEL	DESCRIPTION
Add icon	Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 207 on page 592 for information on the fields. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Add** icon in an entry to add a rule below the current entry. Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action. Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44.11 Dial-in Management

Connect an external serial modem to the **AUX**port to provide a management connection in case the ZyWALL's other WAN connections are down. This is like an auxiliary interface, except it is used for management connections coming into the ZyWALL instead of as a backup WAN connection.

44.11.1 a managementAT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

44.11.2 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the ZyWALL uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

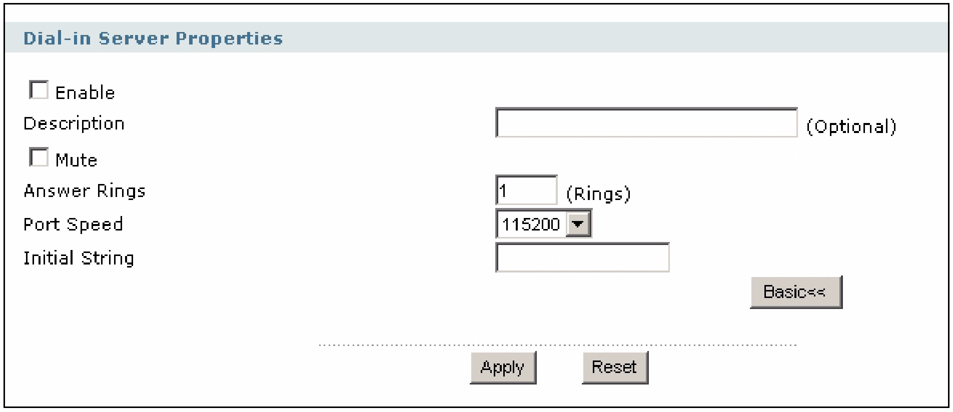
44.11.3 Response Strings

The response strings tell the ZyWALL the tags, or labels, immediately preceding the various call parameters sent from the serial modem. The response strings have not been standardized; please consult the documentation of your serial modem to find the correct tags.

44.12 Dial-in Mgmt Configuration

Click **System** > **Dial-in Mgmt** to display the following screen. Configure this screen for dial-in management connections.

Figure 455 System > Dial-in Mgmt



Dial-in Server Properties

☐ Enable

Description (Optional)

☐ Mute

Answer Rings 1 (Rings)

Port Speed 115200

Initial String

The following table describes the labels in this screen.

Table 213 System > Dial-in Mgmt

LABEL	DESCRIPTION
Enable	Select this check box to turn on dial-in management.
Description	Enter some information about this connection.
Mute	Select this check box to stop the external serial modem from making audible sounds during a dial-in management session.
Answer Rings	Set how many times the ZyWALL lets the incoming dial-in management session ring before processing it.
Port Speed	Use the drop-down list box to select the speed of the connection between the ZyWALL's auxiliary port and the external modem. Available speeds are: **9600**, **19200**, **38400**, **57600**, or **115200** bps.
Initial String	Type the AT command string that the ZyWALL returns to the external serial modem connected to the ZyWALL's auxiliary port during connection initialization. Note: Consult the manual of your external serial modem connected to your ZyWALL's auxiliary port for specific AT commands.
Advanced/Basic	Click **Advanced** to display more configuration fields and edit the details of your dial-in management setup.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

44.13 Vantage CNM

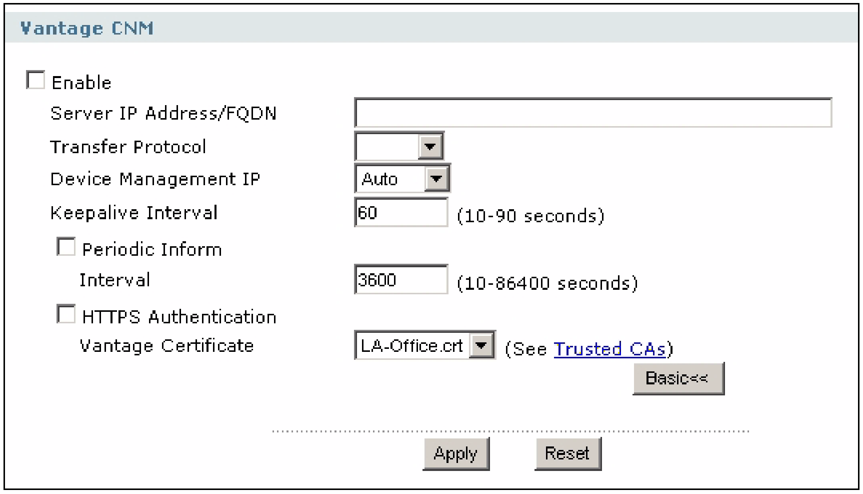
Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyWALL to be managed by the Vantage CNM server, then you should not do any configurations directly to the ZyWALL (using either the web configurator or commands) without notifying the Vantage CNM administrator.

44.14 Configuring Vantage CNM

Vantage CNM is disabled on the device by default. Click **System** > **Vantage CNM** to configure your device's Vantage CNM settings.

Figure 456 System > Vantage CNM



Vantage CNM

☐ Enable

Server IP Address/FQDN

Transfer Protocol

Device Management IP: Auto

Keepalive Interval: 60 (10-90 seconds)

☐ Periodic Inform

Interval: 3600 (10-86400 seconds)

☐ HTTPS Authentication

Vantage Certificate: LA-Office.crt (See Trusted CAs)

The following table describes the labels in this screen.

Table 214 System > Vantage CNM

LABEL	DESCRIPTION
Enable	Select this check box to allow Vantage CNM to manage your ZyWALL.
Server IP Address/ FQDN	Enter the IP address or fully qualified domain name of the Vantage server. If the Vantage CNM server is on a different subnet to the ZyWALL and is behind a NAT router, enter the WAN IP address of the NAT router here and configure the NAT router to forward UDP port 11864 traffic to the Vantage CNM server. If the Vantage CNM server is behind a firewall, you may have to create a rule on the firewall to allow UDP port 11864 traffic through to the Vantage CNM server (most (new) ZyXEL firewalls automatically allow this).
Transfer Protocol	Select whether the Vantage CNM sessions should use regular HTTP connections or secure HTTPS connections. Note: HTTPS is recommended. The Vantage CNM server must use the same setting.
Device Management IP	Select **Auto** to have the ZyWALL allow Vantage CNM sessions to connect to any of the ZyWALL's IP addresses. Select **Custom** to specify the ZyWALL's IP address that allows Vantage CNM sessions. Configure the **Custom IP** field if you select this. You might for example need to specify the IP address when using a WAN trunk that uses multiple WAN IP addresses.
Custom IP	Specify the ZyWALL's IP address that allows Vantage CNM sessions. This field applies when you select **Custom** in the **Device Management IP** field.
Keepalive Interval	Set how often the ZyWALL sends a keep alive packet to the Vantage CNM server if there is no other traffic. The keep alive packets maintain the Vantage CNM server's control session.
Periodic Inform Interval	Select this option to have the ZyWALL periodically send "Inform" messages to the Vantage CNM server.

Table 214 System > Vantage CNM (continued)

LABEL	DESCRIPTION
HTTPS Authentication	When you are using HTTPs, select this option to have the ZyWALL authenticate the Vantage CNM server's certificate. In order to do this you need to import the Vantage CNM server's public key (certificate) into the ZyWALL's trusted certificates.
Vantage Certificate	Select the Vantage CNM server's certificate. This applies when you enable HTTPS authentication.
Advanced/Basic	Click **Advanced** to display more configuration fields or click **Basic** to display fewer fields.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

PART VII

Maintenance & Troubleshooting

File Manager (615)
Logs (625)
Reports (637)
Diagnostics (647)
Reboot (649)
Troubleshooting (651)

45

File Manager

This chapter covers how to use the ZyWALL's **File Manager** screens to handle the ZyWALL's configuration, firmware and shell script files.

45.1 Configuration Files and Shell Scripts Overview

The **File Manager** screens allow you to store multiple configuration files and shell script files.

When you apply a configuration file, the ZyWALL uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the ZyWALL and run when you need them. When you run a shell script, the ZyWALL only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 457 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL applies configuration files differently than it runs shell scripts. This is explained below.

Table 215 Configuration Files and Shell Scripts in the ZyWALL

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the example in Figure 457 on page 615 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

45.1.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ZyWALL treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL exit sub command mode.

“exit” or “!'” must follow sub commands if it is to make the ZyWALL exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

45.1.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL processes the file line-by-line. The ZyWALL checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL still generates a log for any errors.

45.1.3 ZyWALL Configuration File Details

You can store multiple configuration files on the ZyWALL. You can also have the ZyWALL use a different configuration file without the ZyWALL restarting.

- When you first receive the ZyWALL, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ZyWALL creates a **startup-config.conf** file of the current configuration.
- The ZyWALL checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ZyWALL copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.
- When the ZyWALL reboots, if the **startup-config.conf** file passes the error check, the ZyWALL keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

45.1.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the ZyWALL (whether through a management interface or by physically turning the power off and back on), the ZyWALL uses the **system-default.conf** configuration file with the ZyWALL's default settings.

If there is a **startup-config.conf**, the ZyWALL checks it for errors and applies it. If there are no errors, the ZyWALL uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ZyWALL generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL applies the **system-default.conf** configuration file.

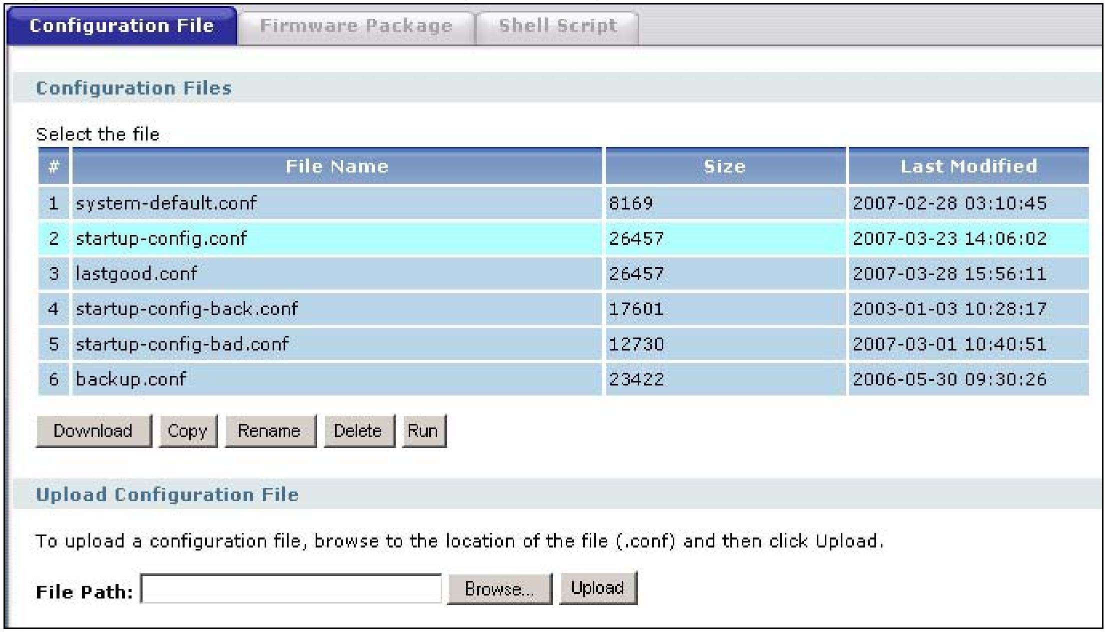
You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL still generates a log for any errors.

45.2 Configuration File Screen

Click **Maintenance** > **File Manager** > **Configuration File** to open the **Configuration File** screen. Use the **Configuration File** screen to store and name configuration files. You can also download configuration files from the ZyWALL to your computer and upload configuration files from your computer to the ZyWALL.

Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Figure 458 Maintenance > File Manager > Configuration File



Select the file

#	File Name	Size	Last Modified
1	system-default.conf	8169	2007-02-28 03:10:45
2	startup-config.conf	26457	2007-03-23 14:06:02
3	lastgood.conf	26457	2007-03-28 15:56:11
4	startup-config-back.conf	17601	2003-01-03 10:28:17
5	startup-config-bad.conf	12730	2007-03-01 10:40:51
6	backup.conf	23422	2006-05-30 09:30:26

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

Do not turn off the ZyWALL while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 216 Maintenance > File Manager > Configuration File

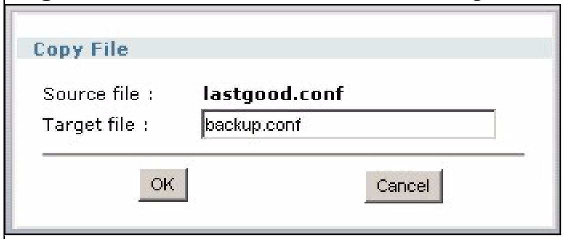
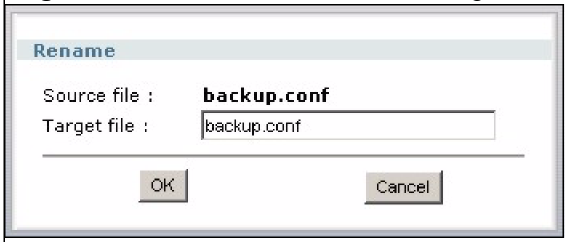
LABEL	DESCRIPTION
Download	Click a configuration file’s row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the ZyWALL. Click a configuration file’s row to select it and click **Copy** to open the **Copy File** screen. **Figure 459** Maintenance > File Manager > Configuration File > Copy  Source file : lastgood.conf Target file : backup.conf Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Rename	Use this button to change the label of a configuration file on the ZyWALL. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the ZyWALL. Click a configuration file’s row to select it and click **Rename** to open the **Rename File** screen. **Figure 460** Maintenance > File Manager > Configuration File > Rename  Source file : backup.conf Target file : backup.conf Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Delete	Click a configuration file’s row to select it and click **Delete** to remove the configuration file from the ZyWALL. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Run	Use this button to have the ZyWALL use a specific configuration file. Click a configuration file’s row to select it and click **Run** to have the ZyWALL use that configuration file. The ZyWALL does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures.

Table 216 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
#	This column displays the number for each configuration file entry. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the ZyWALL's default settings. Select this file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your ZyWALL You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

45.3 Firmware Package Screen

Click **Maintenance > File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the ZyWALL.

The web configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

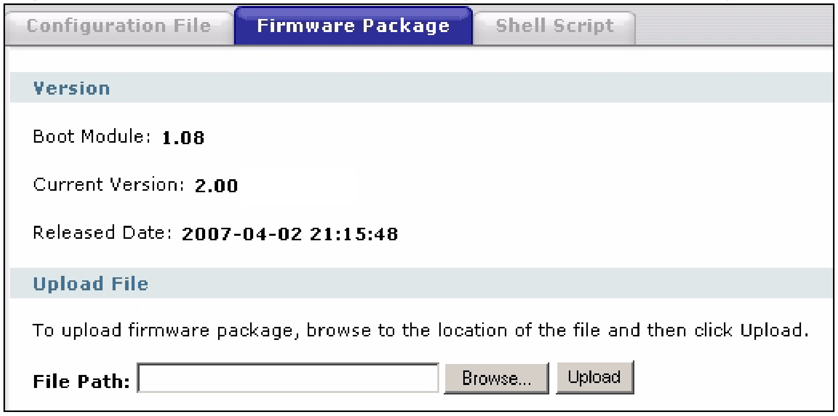
Find the firmware package at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin".

The ZyWALL's firmware package cannot go through the ZyWALL when you enable the anti-virus **Destroy compressed files that could not be decompressed** option. The ZyWALL classifies the firmware package as not being able to be decompressed and deletes it. You can upload the firmware package to the ZyWALL with the option enabled, so you only need to clear the **Destroy compressed files that could not be decompressed** option while you download the firmware package. See Section 28.3.1 on page 408 for more on the anti-virus **Destroy compressed files that could not be decompressed** option.

The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL while the firmware update is in progress!

The ZyWALL automatically reboots after a successful upload.

Figure 461 Maintenance > File Manager > Firmware Package



Boot Module: 1.08

Current Version: 2.00

Released Date: 2007-04-02 21:15:48

To upload firmware package, browse to the location of the file and then click Upload.

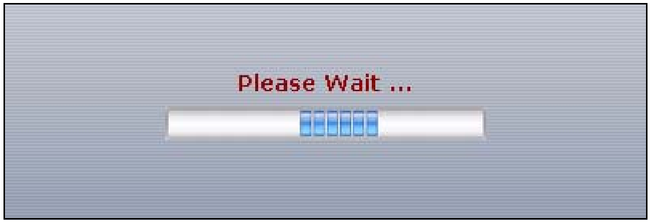
The following table describes the labels in this screen.

Table 217 Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the ZyWALL.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

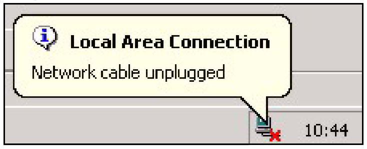
Figure 462 Firmware Upload In Process



Please Wait ...

The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 463 Network Temporarily Disconnected



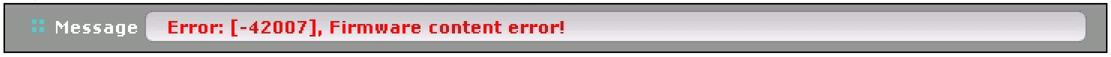
Local Area Connection

Network cable unplugged

After five minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

Figure 464 Firmware Upload Error



Error: [-42007], Firmware content error!

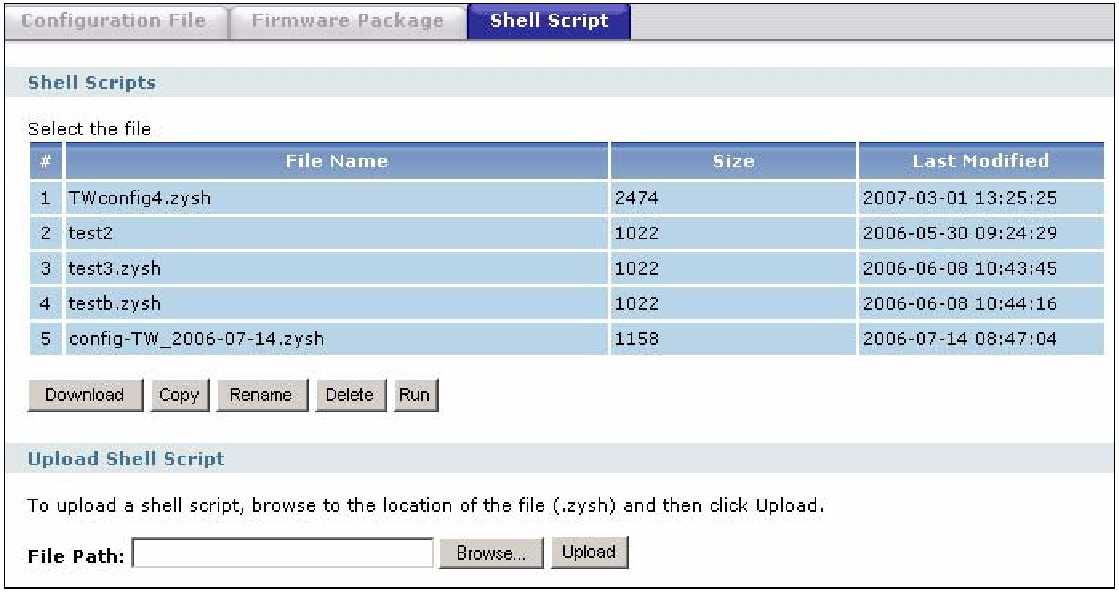
45.4 Shell Script Screen

Use shell script files to have the ZyWALL use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance** > **File Manager** > **Shell Script** to open the **Shell Script** screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the ZyWALL at the same time.

You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the ZyWALL restarts. You could multiple `write` commands in a long script.

Figure 465 Maintenance > File Manager > Shell Script



Shell Scripts

Select the file

#	File Name	Size	Last Modified
1	TWconfig4.zysh	2474	2007-03-01 13:25:25
2	test2	1022	2006-05-30 09:24:29
3	test3.zysh	1022	2006-06-08 10:43:45
4	testb.zysh	1022	2006-06-08 10:44:16
5	config-TW_2006-07-14.zysh	1158	2006-07-14 08:47:04

Upload Shell Script

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

File Path:

Each field is described in the following table.

Table 218 Maintenance > File Manager > Shell Script

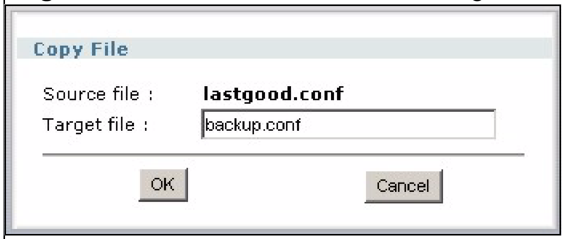
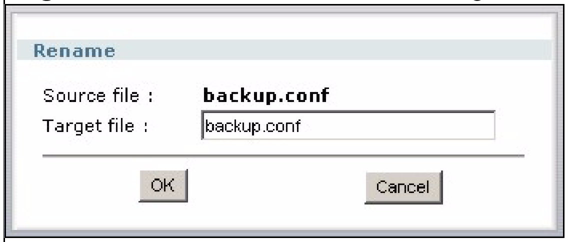
LABEL	DESCRIPTION
Download	Click a shell script file’s row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the ZyWALL. Click a shell script file’s row to select it and click **Copy** to open the **Copy File** screen. **Figure 466** Maintenance > File Manager > Shell Script > Copy  Copy File Source file : lastgood.conf Target file : backup.conf Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 218 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the ZyWALL. You cannot rename a shell script to the name of another shell script in the ZyWALL. Click a shell script’s row to select it and click **Rename** to open the **Rename File** screen. **Figure 467** Maintenance > File Manager > Shell Script > Rename  Source file : **backup.conf** Target file : backup.conf Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Delete	Click a shell script file’s row to select it and click **Delete** to delete the shell script file from the ZyWALL. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Run	Use this button to have the ZyWALL use a specific shell script file. Click a shell script file’s row to select it and click **Run** to have the ZyWALL use that shell script file. You may need to wait awhile for the ZyWALL to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your ZyWALL.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

46

Logs

This chapter provides general information about the ZyWALL’s log feature. See Appendix B on page 663 for individual log descriptions.

The following table displays the maximum number of system log messages in the ZyWALL.

Table 219 Specifications: Logs

LABEL	DESCRIPTION
Maximum Number of Log Messages (System Log)	512
Maximum Number of Log Messages (Debug Log)	1024

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

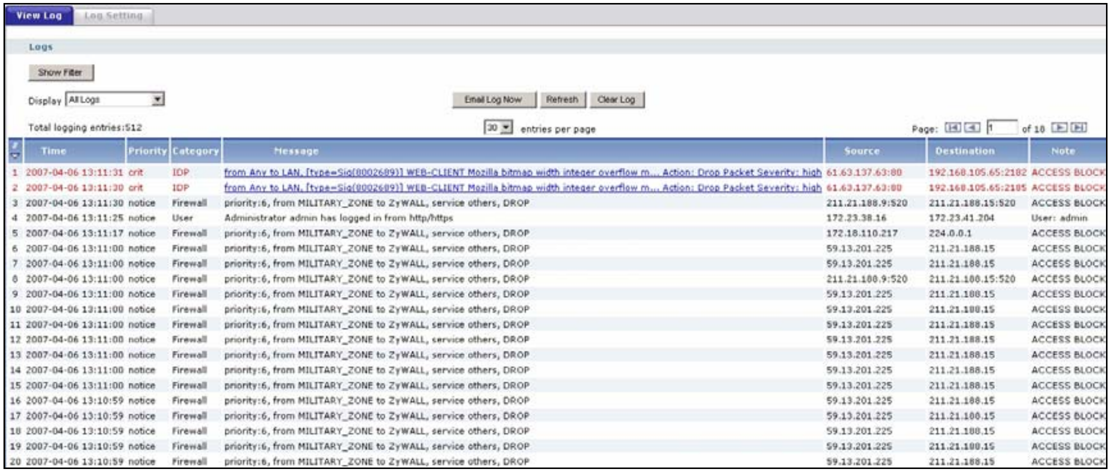
46.1 View Log Screen

The **View Log** screen displays the current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, firewall or user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click **Maintenance** > **Log**. The log is displayed in the following screen.

Figure 468 Maintenance > Log > View Log



Display: All Logs

Total logging entries:512

30 entries per page

Page: 1 of 18

```
#  Time                Priority Category Message                                                                                                    Source            Destination           Note
1  2007-04-06 13:11:31 crit     IDP      from Any to LAN, [type=Sig(8002689)] WEB-CLIENT Mozilla bitmap width integer overflow m... Action: Drop Packet Severity: high 61.63.137.63:80    192.168.105.65:2182   ACCESS BLOCK
2  2007-04-06 13:11:30 crit     IDP      from Any to LAN, [type=Sig(8002689)] WEB-CLIENT Mozilla bitmap width integer overflow m... Action: Drop Packet Severity: high 61.63.137.63:80    192.168.105.65:2185   ACCESS BLOCK
3  2007-04-06 13:11:30 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               211.21.188.9:520  211.21.188.15:520     ACCESS BLOCK
4  2007-04-06 13:11:25 notice   User     Administrator admin has logged in from http/https                                                          172.23.38.16      172.23.41.204         User: admin
5  2007-04-06 13:11:17 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               172.18.110.217    224.0.0.1             ACCESS BLOCK
6  2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
7  2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
8  2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               211.21.188.9:520  211.21.188.15:520     ACCESS BLOCK
9  2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
10 2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
11 2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
12 2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
13 2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
14 2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
15 2007-04-06 13:11:00 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
16 2007-04-06 13:10:59 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
17 2007-04-06 13:10:59 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
18 2007-04-06 13:10:59 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
19 2007-04-06 13:10:59 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
20 2007-04-06 13:10:59 notice   Firewall priority:6, from MILITARY_ZONE to ZyWALL, service others, DROP                                               59.13.201.225     211.21.188.15         ACCESS BLOCK
```

If an event generates log messages and alerts, it is displayed in red. Otherwise, it is displayed in black. The following table describes the labels in this screen.

Table 220 Maintenance > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Service**, **Keyword**, and **Search** fields are available.
No Filter	These fields are displayed when you hide the filter.
Display	Select the log(s) you want to view. You can also view **All Logs** on one screen, or you can view the **Debug Log**. The screen is updated right after you change the selection.
Email Log Now	Click this button to send the selected log message(s) to the **Active** e-mail address(es) specified in the **Send Log To** field on the **Log Settings** page. (See Section 46.3 on page 628 or Section 46.3.1 on page 629 for more information about these fields.)
Refresh	Click this button to update the information on the log screen.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
Filter	These fields are displayed when you show the filter. When the filter is shown, the filter criteria are not applied until you click the **Search** button.
Display	Select the log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This field is read-only if the **Category** is **Debug Log**. Select the lowest-priority log messages you would like to see. The log will display every log message with this priority or higher. Choices are: **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority.
Source Address	Type the IP address of the source of the incoming packet when the log message was generated. Do not include the port in this filter.
Destination Address	Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Service	Select the service whose log messages you would like to see. The web configurator uses the protocol and destination port number(s) of the service to select which log messages you see.

Table 220 Maintenance > Log > View Log (continued)

LABEL	DESCRIPTION
Keyword	Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Search	Click this button to update the log using the current filter settings.
Total Logging Entries	This is the number of logs recorded in the ZyWALL.
entries per page	Select the number of log messages you would like to see on one screen. Choices are: **30**, **50**, and **80**.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on (see **Log Consolidation** in Table 222 on page 631) and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

The Web configurator saves the filter settings if you leave the **View Log** screen and return to it later.

46.2 Log Settings Screens

The **Log Settings** screens control log messages and alerts. A log message stores the information for viewing (for example, in the **View Log** tab) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The ZyWALL provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** tab, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Settings** tab also controls what information is saved in each log. For the system log, you can also specify which log messages is e-mailed, where it is e-mailed, and how often it is e-mailed.

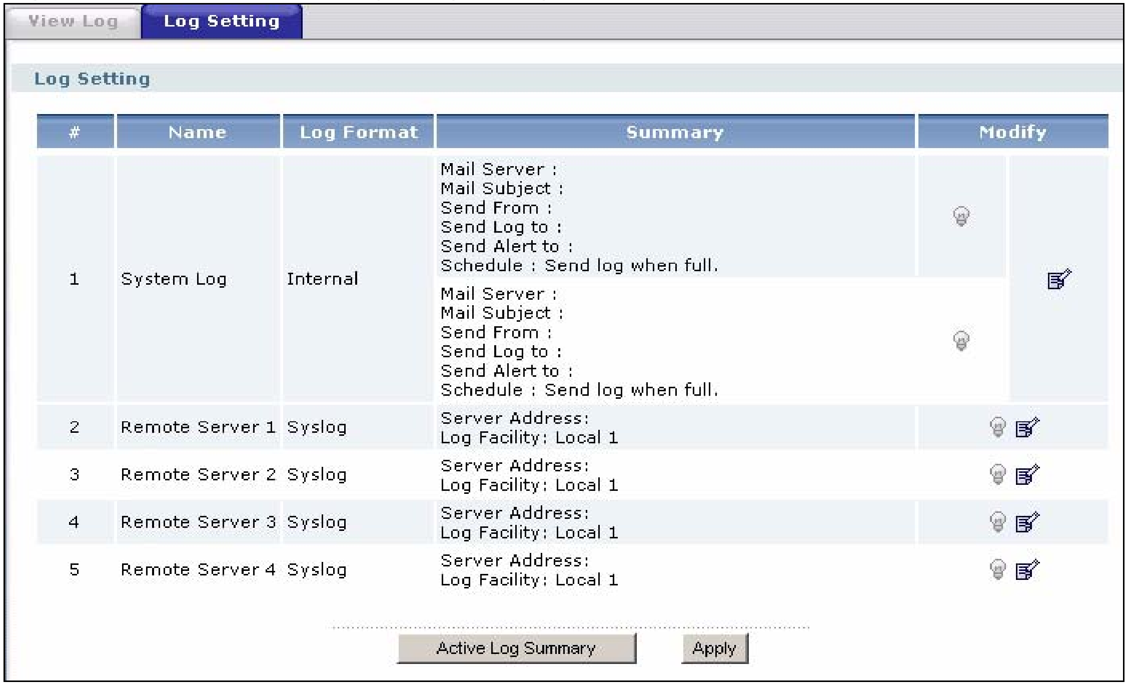
For alerts, the **Log Settings** tab controls which events generate alerts and where alerts are e-mailed.

The **Log Settings Summary** screen provides a summary of all the settings. You can use the **Log Settings Edit** screen to maintain the detailed settings (such as log categories, e-mail addresses, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

46.3 Log Settings Summary

To access this screen, click **Maintenance** > **Log** > **Log Setting**.

Figure 469 Maintenance > Log > Log Setting



#	Name	Log Format	Summary	Modify
1	System Log	Internal	Mail Server : Mail Subject : Send From : Send Log to : Send Alert to : Schedule : Send log when full. Mail Server : Mail Subject : Send From : Send Log to : Send Alert to : Schedule : Send log when full.	
2	Remote Server 1	Syslog	Server Address: Log Facility: Local 1	
3	Remote Server 2	Syslog	Server Address: Log Facility: Local 1	
4	Remote Server 3	Syslog	Server Address: Log Facility: Local 1	
5	Remote Server 4	Syslog	Server Address: Log Facility: Local 1	

The following table describes the labels in this screen.

Table 221 Maintenance > Log > Log Setting

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific log.
Name	This field displays the name of the log (system log or one of the remote servers).
Log Format	This field displays the format of the log. Formats are **Internal** and **Syslog**. **Internal** - system log; you can view the log on the **View Log** tab. **Syslog** - syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 46.3.1 on page 629 for more information.

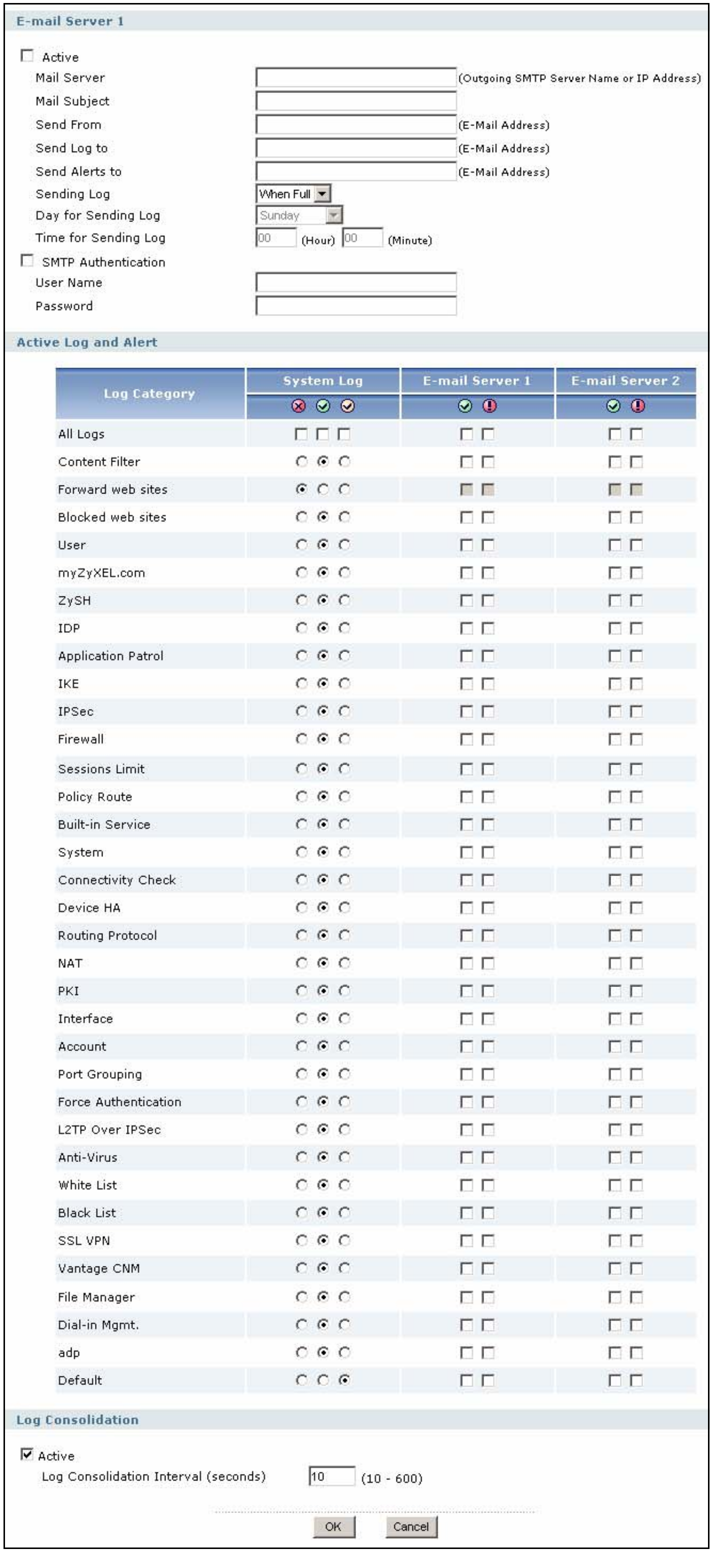
Table 221 Maintenance > Log > Log Setting (continued)

LABEL	DESCRIPTION
Modify	This column provides icons to activate or deactivate logs and to modify the settings. To activate or deactivate a log, click the **Active** icon. Make sure you click **Apply** to save and apply the change. To edit the settings, click the **Edit** icon next to the associated log. The **Log Settings Edit** screen appears.
Active Log Summary	Click this button to open the **Active Log Summary Edit** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

46.3.1 Log Settings Edit E-mail

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the **Log Settings Summary** screen (see Section 46.3 on page 628), and click the appropriate **Edit** icon.

Figure 470 Maintenance > Log > Log Setting > E-mail > Edit



E-mail Server 1

☐ Active
Mail Server (Outgoing SMTP Server Name or IP Address)
Mail Subject
Send From (E-Mail Address)
Send Log to (E-Mail Address)
Send Alerts to (E-Mail Address)
Sending Log: When Full
Day for Sending Log: Sunday
Time for Sending Log: 00 (Hour) 00 (Minute)
☐ SMTP Authentication
User Name
Password

Active Log and Alert

Log Category	System Log			E-mail Server 1		E-mail Server 2	
	⊗	✓	✓	✓	!	✓	!
All Logs	☐	☐	☐	☐	☐	☐	☐
Content Filter	○	●	○	☐	☐	☐	☐
Forward web sites	●	○	○	☐	☐	☐	☐
Blocked web sites	○	●	○	☐	☐	☐	☐
User	○	●	○	☐	☐	☐	☐
myZyXEL.com	○	●	○	☐	☐	☐	☐
ZySH	○	●	○	☐	☐	☐	☐
IDP	○	●	○	☐	☐	☐	☐
Application Patrol	○	●	○	☐	☐	☐	☐
IKE	○	●	○	☐	☐	☐	☐
IPSec	○	●	○	☐	☐	☐	☐
Firewall	○	●	○	☐	☐	☐	☐
Sessions Limit	○	●	○	☐	☐	☐	☐
Policy Route	○	●	○	☐	☐	☐	☐
Built-in Service	○	●	○	☐	☐	☐	☐
System	○	●	○	☐	☐	☐	☐
Connectivity Check	○	●	○	☐	☐	☐	☐
Device HA	○	●	○	☐	☐	☐	☐
Routing Protocol	○	●	○	☐	☐	☐	☐
NAT	○	●	○	☐	☐	☐	☐
PKI	○	●	○	☐	☐	☐	☐
Interface	○	●	○	☐	☐	☐	☐
Account	○	●	○	☐	☐	☐	☐
Port Grouping	○	●	○	☐	☐	☐	☐
Force Authentication	○	●	○	☐	☐	☐	☐
L2TP Over IPSec	○	●	○	☐	☐	☐	☐
Anti-Virus	○	●	○	☐	☐	☐	☐
White List	○	●	○	☐	☐	☐	☐
Black List	○	●	○	☐	☐	☐	☐
SSL VPN	○	●	○	☐	☐	☐	☐
Vantage CNM	○	●	○	☐	☐	☐	☐
File Manager	○	●	○	☐	☐	☐	☐
Dial-in Mgmt.	○	●	○	☐	☐	☐	☐
adp	○	●	○	☐	☐	☐	☐
Default	○	○	●	☐	☐	☐	☐

Log Consolidation

☑ Active
Log Consolidation Interval (seconds): 10 (10 - 600)

The following table describes the labels in this screen.

Table 222 Maintenance > Log > Log Setting > E-mail > Edit

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: **When Full**, **Hourly**, **Daily**, and **Weekly**.
Day for Sending Log	This field is available if the log is e-mailed **Weekly**. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed **Weekly** or **Daily**. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Active Log and Alert	
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category** (except **All Logs**; see below). There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - create log messages and alerts from this category **enable all logs** (yellow checkmark) - create log messages, alerts, and debugging information from this category; the ZyWALL does not e-mail debugging information, however, even if this setting is selected. If you select one of the check boxes for **All Logs**, it affects the settings for every category.
E-mail Server 1	Select whether this category of events should be included in the log messages when it is e-mailed (green checkmark) and/or in alerts (yellow exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether this category of events should be included in log messages when it is e-mailed (green checkmark) and/or in alerts (yellow exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**.

Table 222 Maintenance > Log > Log Setting > E-mail > Edit (continued)

LABEL	DESCRIPTION
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

46.3.2 Log Settings Edit syslog

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see Section 46.3 on page 628), and click the appropriate **Edit** icon.

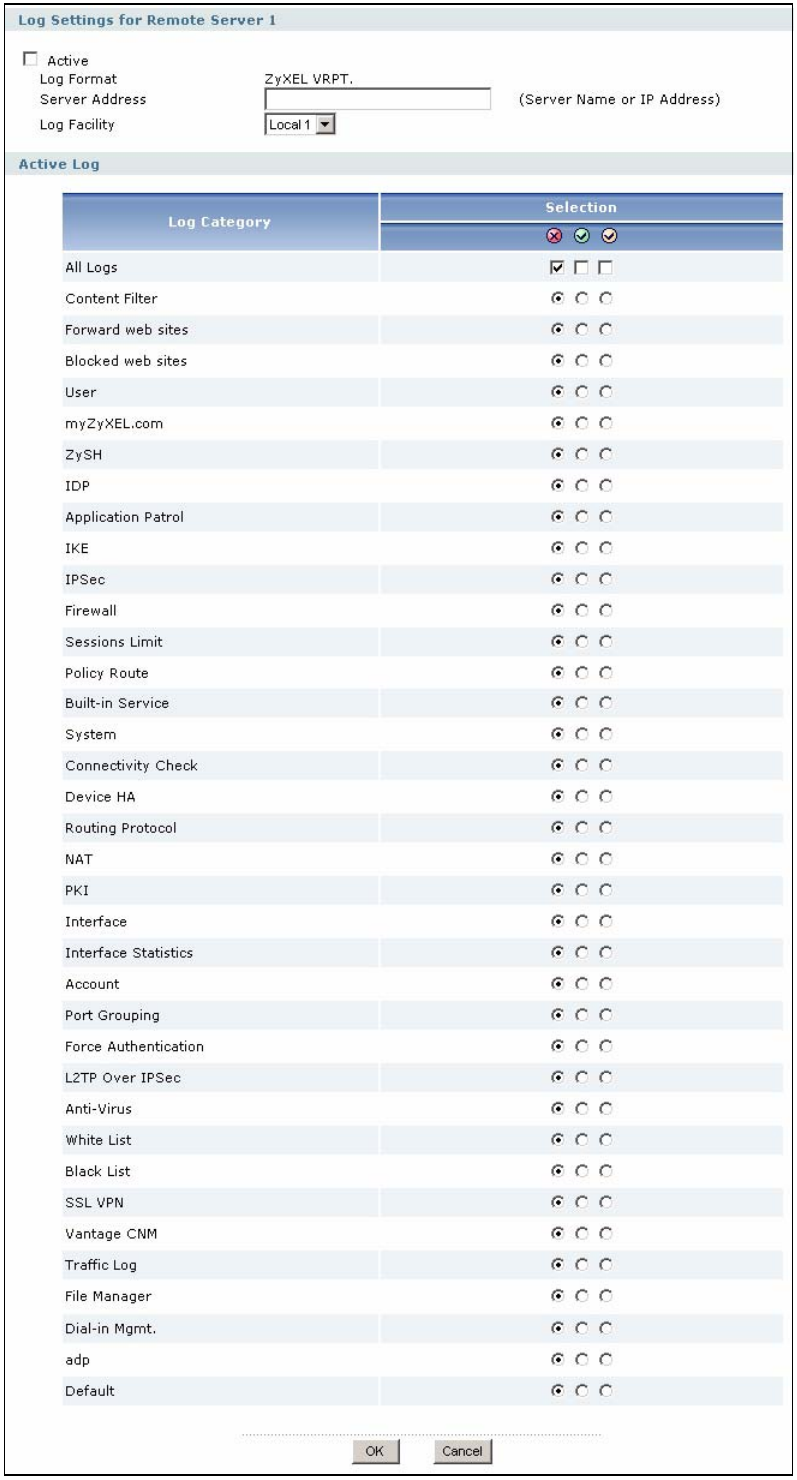


Figure 471 Maintenance > Log > Log Setting > Remote Server > Edit

Log Settings for Remote Server 1

☐ Active
Log Format: ZyXEL VRPT.
Server Address: (Server Name or IP Address)
Log Facility: Local 1

Active Log

Log Category	Selection		
	⊗	✓	✓
All Logs	☑	☐	☐
Content Filter	●	○	○
Forward web sites	●	○	○
Blocked web sites	●	○	○
User	●	○	○
myZyXEL.com	●	○	○
ZySH	●	○	○
IDP	●	○	○
Application Patrol	●	○	○
IKE	●	○	○
IPSec	●	○	○
Firewall	●	○	○
Sessions Limit	●	○	○
Policy Route	●	○	○
Built-in Service	●	○	○
System	●	○	○
Connectivity Check	●	○	○
Device HA	●	○	○
Routing Protocol	●	○	○
NAT	●	○	○
PKI	●	○	○
Interface	●	○	○
Interface Statistics	●	○	○
Account	●	○	○
Port Grouping	●	○	○
Force Authentication	●	○	○
L2TP Over IPSec	●	○	○
Anti-Virus	●	○	○
White List	●	○	○
Black List	●	○	○
SSL VPN	●	○	○
Vantage CNM	●	○	○
Traffic Log	●	○	○
File Manager	●	○	○
Dial-in Mgmt.	●	○	○
adp	●	○	○
Default	●	○	○

The following table describes the labels in this screen.

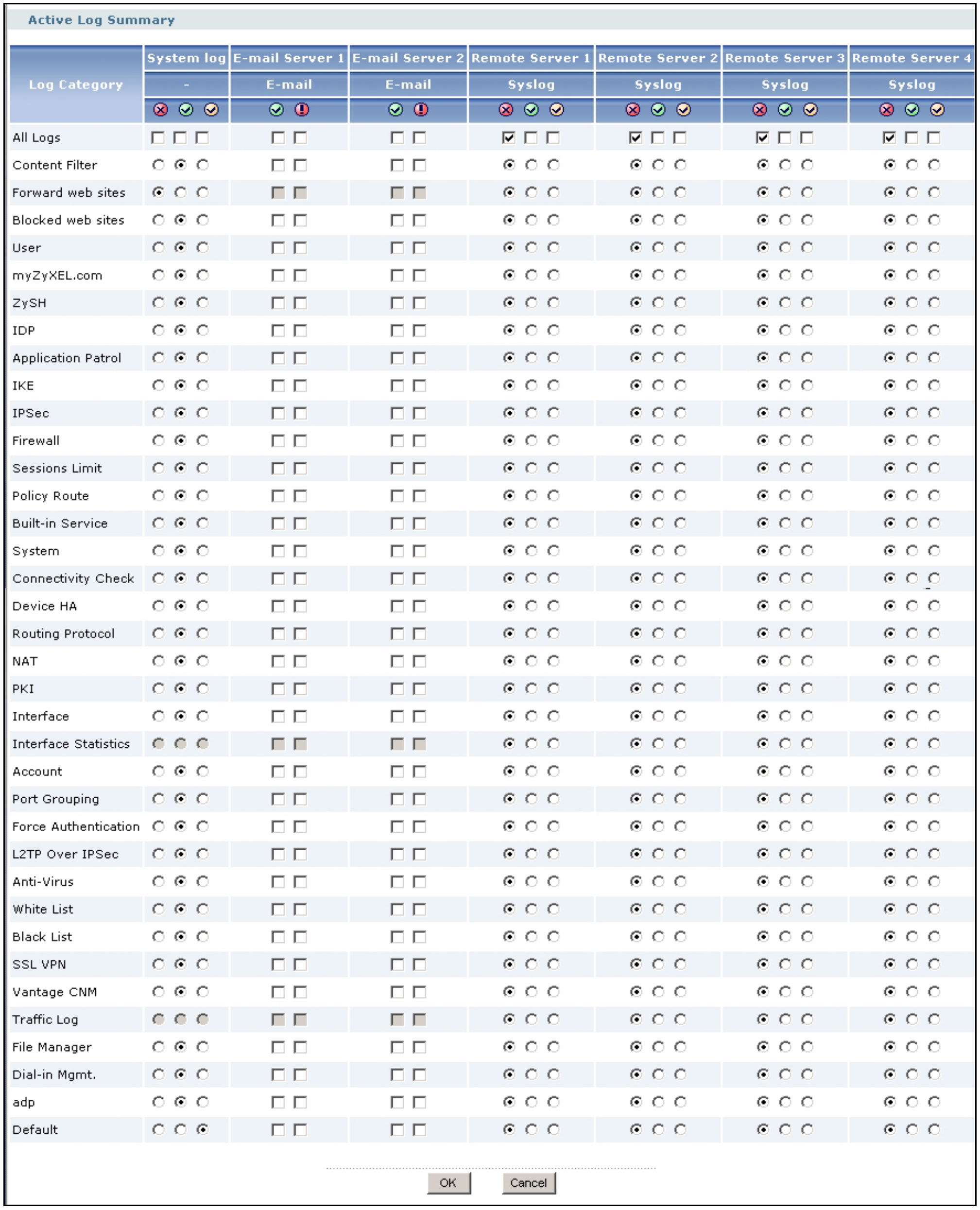
Table 223 Maintenance > Log > Log Setting > Remote Server > Edit

LABEL	DESCRIPTION
Log Settings for Remote Server 1	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **Internal** - system log; you can view the log on the **View Log** tab. **ZyXEL VRPT** - syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable all logs** (yellow checkmark) - log regular information, alerts, and debugging information from this category If you check one of the check boxes for **All Logs**, it affects the settings for every category.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

46.3.3 Active Log Summary

The **Active Log Summary** screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names).To access this screen, go to the **Log Settings Summary** screen (see Section 46.3 on page 628), and click the **Active Log Summary** button.

Figure 472 Active Log Summary



Active Log Summary

Log Category	System log	E-mail Server 1	E-mail Server 2	Remote Server 1	Remote Server 2	Remote Server 3	Remote Server 4
	-	E-mail	E-mail	Syslog	Syslog	Syslog	Syslog
	✗ ✓ ✓	✓ !	✓ !	✗ ✓ ✓	✗ ✓ ✓	✗ ✓ ✓	✗ ✓ ✓
All Logs	☐ ☐ ☐	☐ ☐	☐ ☐	☑ ☐ ☐	☑ ☐ ☐	☑ ☐ ☐	☑ ☐ ☐
Content Filter	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Forward web sites	● ○ ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Blocked web sites	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
User	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
myZyXEL.com	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
ZySH	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
IDP	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Application Patrol	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
IKE	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
IPSec	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Firewall	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Sessions Limit	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Policy Route	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Built-in Service	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
System	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Connectivity Check	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Device HA	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Routing Protocol	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
NAT	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
PKI	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Interface	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Interface Statistics	○ ○ ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Account	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Port Grouping	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Force Authentication	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
L2TP Over IPSec	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Anti-Virus	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
White List	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Black List	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
SSL VPN	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Vantage CNM	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Traffic Log	○ ○ ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
File Manager	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Dial-in Mgmt.	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
adp	○ ● ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
Default	○ ○ ●	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○

This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 46.3.1 on page 629, where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 224 Maintenance > Log > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.

Table 224 Maintenance > Log > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable all logs** (yellow checkmark) - log regular information, alerts, and debugging information from this category If you check one of the check boxes for **All Logs**, it affects the settings for every category.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

47

Reports

This chapter provides information about the report screens.

47.1 Traffic Screen

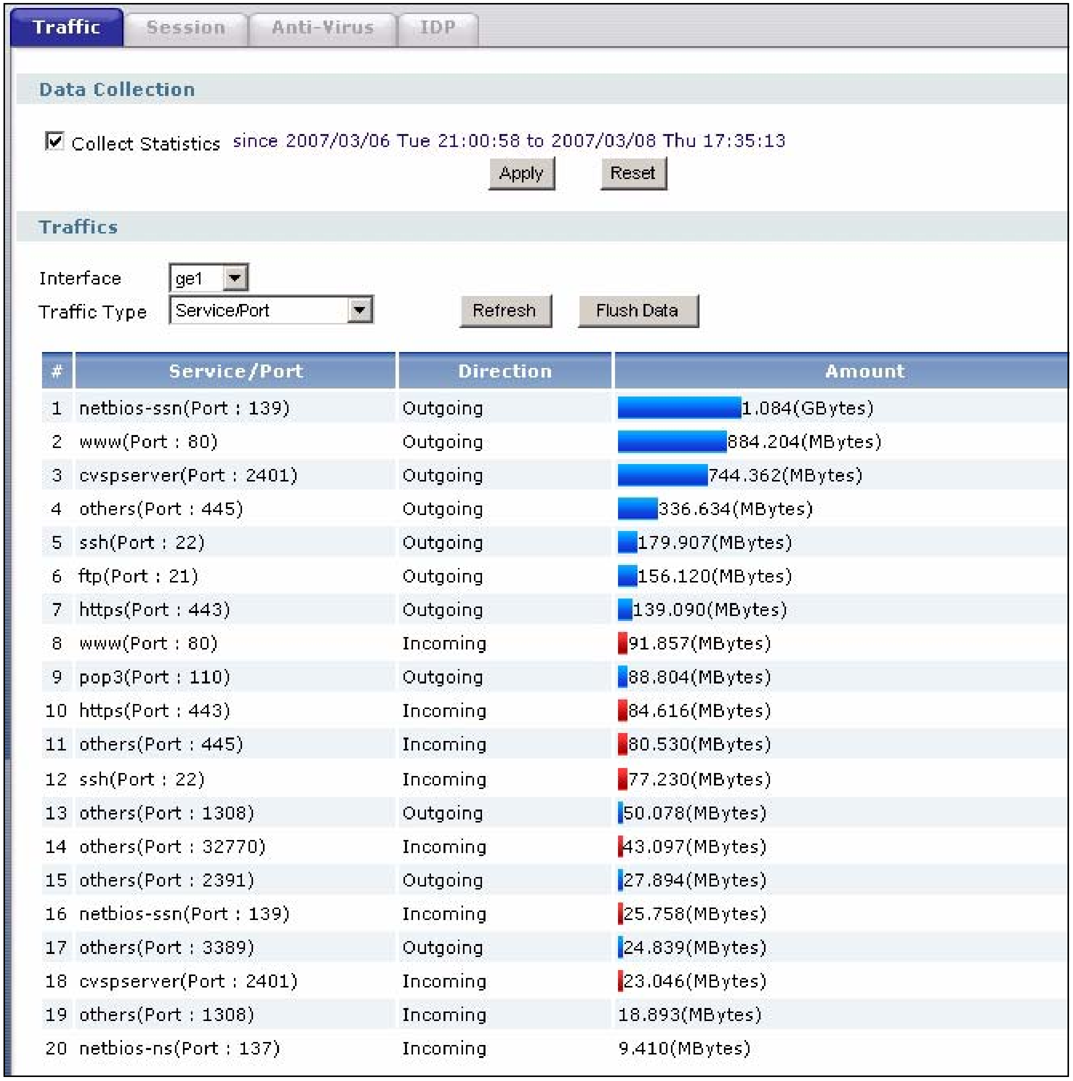
Click **Maintenance** > **Report** > **Traffic** to display the **Traffic** screen. The **Traffic** screen provides basic information about the following metrics:

- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the ZyWALL counts HTTP GET packets. Please see Table 225 on page 638 for more information.
- Most-used protocols or service ports and the amount of traffic on each one
- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

The reporting may decrease the overall throughput through the ZyWALL.

You use the **Traffic** screen to tell the ZyWALL when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the **Traffic** screen.

Figure 473 Maintenance > Report > Traffic



Data Collection

☑ Collect Statistics since 2007/03/06 Tue 21:00:58 to 2007/03/08 Thu 17:35:13

Traffics

Interface: ge1

Traffic Type: Service/Port

#	Service/Port	Direction	Amount
1	netbios-ssn(Port : 139)	Outgoing	1.084(GBytes)
2	www(Port : 80)	Outgoing	884.204(MBytes)
3	cvspserver(Port : 2401)	Outgoing	744.362(MBytes)
4	others(Port : 445)	Outgoing	336.634(MBytes)
5	ssh(Port : 22)	Outgoing	179.907(MBytes)
6	ftp(Port : 21)	Outgoing	156.120(MBytes)
7	https(Port : 443)	Outgoing	139.090(MBytes)
8	www(Port : 80)	Incoming	91.857(MBytes)
9	pop3(Port : 110)	Outgoing	88.804(MBytes)
10	https(Port : 443)	Incoming	84.616(MBytes)
11	others(Port : 445)	Incoming	80.530(MBytes)
12	ssh(Port : 22)	Incoming	77.230(MBytes)
13	others(Port : 1308)	Outgoing	50.078(MBytes)
14	others(Port : 32770)	Incoming	43.097(MBytes)
15	others(Port : 2391)	Outgoing	27.894(MBytes)
16	netbios-ssn(Port : 139)	Incoming	25.758(MBytes)
17	others(Port : 3389)	Outgoing	24.839(MBytes)
18	cvspserver(Port : 2401)	Incoming	23.046(MBytes)
19	others(Port : 1308)	Incoming	18.893(MBytes)
20	netbios-ns(Port : 137)	Incoming	9.410(MBytes)

There is a limit on the number of records shown in the report. Please see Table 226 on page 640 for more information. The following table describes the labels in this screen.

Table 225 Maintenance > Report > Traffic

LABEL	DESCRIPTION
Data Collection	
Collect Statistics	Select this to have the ZyWALL collect data for the report. If the ZyWALL has already been collecting data, the collection period displays to the right. The progress is not tracked here real-time, but you can click the **Refresh** button to update it.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.
Traffics	
Interface	Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge, PPPoE/PPTP, and auxiliary interfaces.

Table 225 Maintenance > Report > Traffic (continued)

LABEL	DESCRIPTION
Traffic Type	Select the type of report to display. Choices are: **Host IP Address/User** - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one. **Service/Port** - displays the most-used protocols or service ports and the amount of traffic for each one. **Web Site Hits** - displays the most-visited Web sites and how many times each one has been visited. Each type of report has different information in the report (below).
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard the report data for the selected interface and update the report display.
	These fields are available when the **Traffic Type** is **Host IP Address/User**.
#	This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic.
IP Address/ User	This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 226 on page 640.
Direction	This field indicates whether the IP address or user is sending or receiving traffic. Choices are **Incoming** and **Outgoing**. **Incoming** - traffic is coming from the IP address or user to the ZyWALL. **Outgoing** - traffic is going from the ZyWALL to the IP address or user.
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. If the **Direction** is **Incoming**, a red bar is displayed; if the **Direction** is **Outgoing**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 226 on page 640.
	These fields are available when the **Traffic Type** is **Service/Port**.
#	This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic.
Service/Port	This field displays the protocol or service port in this record. The maximum number of protocols or service ports in this report is indicated in Table 226 on page 640.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. Choices are **Incoming** and **Outgoing**. **Incoming** - traffic is coming into the router through the interface **Outgoing** - traffic is going out from the router through the interface
Amount	This field displays how much traffic was sent or received from the indicated service / port. If the **Direction** is **Incoming**, a red bar is displayed; if the **Direction** is **Outgoing**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 226 on page 640.
	These fields are available when the **Traffic Type** is **Web Site Hits**.
#	This field is the rank of each record. The domain names are sorted by the number of hits.

Table 225 Maintenance > Report > Traffic (continued)

LABEL	DESCRIPTION
Web Site	This field displays the domain names most often visited. The ZyWALL counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 226 on page 640.
Hits	This field displays how many hits the Web site received. The ZyWALL counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the ZyWALL counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 226 on page 640.

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

Table 226 Maximum Values for Reports

LABEL	DESCRIPTION
Maximum Number of Records	20
Byte Count Limit	2^{64} bytes; this is just less than 17 million terabytes.
Hit Count Limit	2^{64} hits; this is over 1.8×10^{19} hits.

47.2 Session Screen

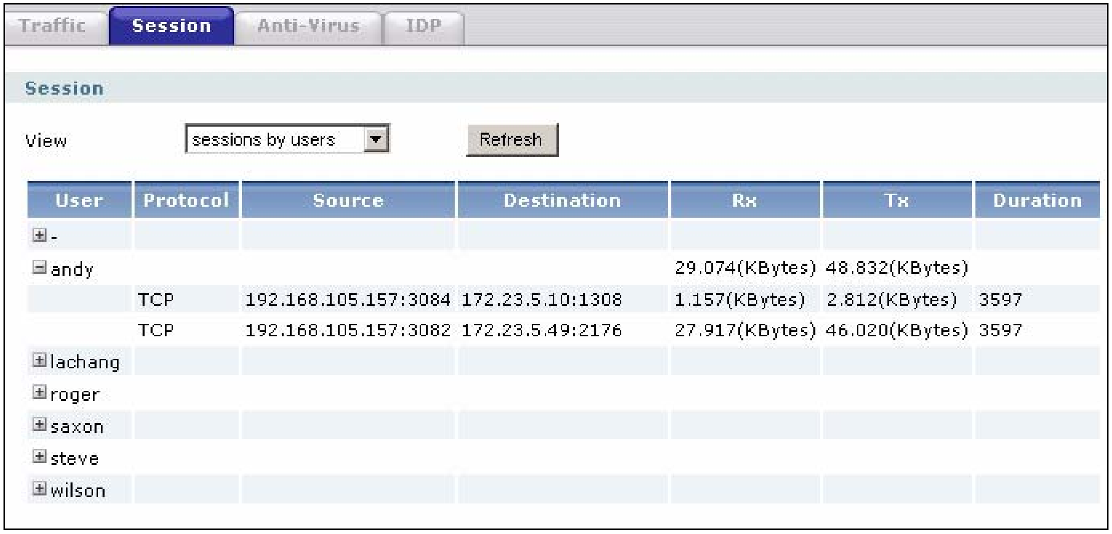
The **Session** screen displays information about active sessions for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all the active sessions by user or by service, or you can filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

To access this screen, login to the web configurator. When the main screen appears, click **Maintenance** > **Report** > **Session**. The following screen appears.

Figure 474 Maintenance > Report > Session



User	Protocol	Source	Destination	Rx	Tx	Duration
⊞ -						
⊟ andy				29.074(KBytes)	48.832(KBytes)	
	TCP	192.168.105.157:3084	172.23.5.10:1308	1.157(KBytes)	2.812(KBytes)	3597
	TCP	192.168.105.157:3082	172.23.5.49:2176	27.917(KBytes)	46.020(KBytes)	3597
⊞ lachang						
⊞ roger						
⊞ saxon						
⊞ steve						
⊞ wilson						

The following table describes the labels in this screen.

Table 227 Maintenance > Report > Session

LABEL	DESCRIPTION
View	Select how you want the information to be displayed. Choices are: **sessions by users** - display all active sessions by user **sessions by services** - display all active sessions by service or protocol **all sessions** - filter the active sessions by the **User**, **Service**, **Source Address**, and **Destination Address**, and display them by user. The **User**, **Service**, **Source Address**, and **Destination Address** fields are only available when **all sessions** is selected.
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
	The **User**, **Service**, **Source Address**, and **Destination Address** fields have no effect until you click the **Search** button, even if you click the **Refresh** button.
User	This field is only available when **all sessions** is selected. Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name.
Service	This field is only available when **all sessions** is selected. Select the service or service group whose sessions you want to view. The ZyWALL identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined. (See Chapter 36 on page 521 for more information about services.)
Source Address	This field is only available when **all sessions** is selected. Type the source IP address whose sessions you want to view. You cannot include the source port.
Destination Address	This field is only available when **all sessions** is selected. Type the destination IP address whose sessions you want to view. You cannot include the destination port.
Search	Click this button to update the information on the screen using the filter criteria in the **User**, **Service**, **Source Address**, and **Destination Address** fields.
sessions per page	Select the number of active sessions displayed on each page. You can use the arrow keys on the right to change pages.
User	This field displays the user in each active session. If you are looking at the **sessions by users** or **all sessions** report, click the blue plus sign (+) next to each user to look at detailed session information by protocol.

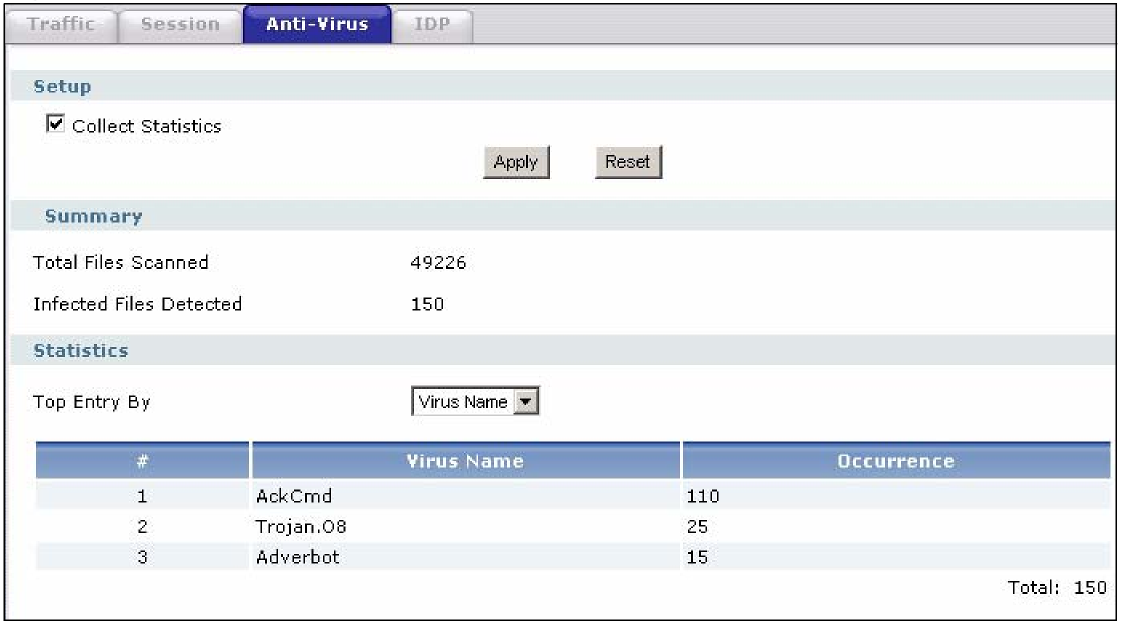
Table 227 Maintenance > Report > Session (continued)

LABEL	DESCRIPTION
Protocol Service	This field displays the protocol used in each active session. If you are looking at the **sessions by services** report, click the blue plus sign (+) next to each protocol to look at detailed session information by user.
Source	This field displays the source IP address and port in each active session.
Destination	This field displays the destination IP address and port in each active session.
Rx	This field displays the amount of information received by the source in the active session.
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.

47.3 Anti-Virus Report Screen

Click **Maintenance** > **Report** > **Anti-Virus** to display the following screen. This screen displays anti-virus statistics.

Figure 475 Maintenance > Report > Anti-Virus: Virus Name



Setup

☑ Collect Statistics

Summary

Total Files Scanned 49226

Infected Files Detected 150

Statistics

Top Entry By: Virus Name

#	Virus Name	Occurrence
1	AckCmd	110
2	Trojan.O8	25
3	Adverbot	15

Total: 150

The following table describes the labels in this screen.

Table 228 Maintenance > Report > Anti-Virus

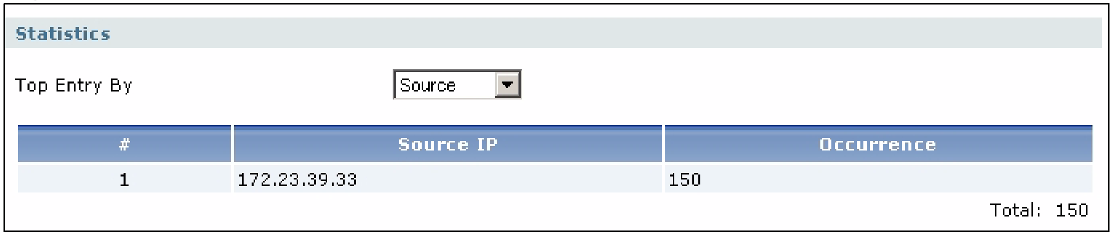
LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the ZyWALL collect anti-virus statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click the **Flush** button. Collecting starts over and a new collection start time displays.
Total Files Scanned	This field displays the number of files that the ZyWALL has scanned for viruses.

Table 228 Maintenance > Report > Anti-Virus (continued)

LABEL	DESCRIPTION
Infected Files Detected	This field displays the number of files in which the ZyWALL has detected a virus.
Top Entry By	Use this field to have the following (read-only) table display the top anti-virus entries by **Virus Name**, **Source** or **Destination**. Select **Virus Name** to list the most common viruses that the ZyWALL has detected. Select **Source** to list the source IP addresses from which the ZyWALL has detected the most virus-infected files. Select **Destination** to list the most common destination IP addresses for virus-infected files that ZyWALL has detected.
#	This field displays the entry's rank in the list of the top entries.
Virus name	This column displays when you display the entries by **Virus Name**. This displays the name of a detected virus.
Source IP	This column displays when you display the entries by **Source.** It shows the source IP address of virus-infected files that the ZyWALL has detected.
Destination IP	This column displays when you display the entries by **Destination.** It shows the destination IP address of virus-infected files that the ZyWALL has detected.
Occurrences	This field displays how many times the ZyWALL has detected the event described in the entry.
Total	This field displays the sum of the occurrences of the events in the entries.

The statistics display as follows when you display the top entries by source.

Figure 476 Maintenance > Report > Anti-Virus: Source

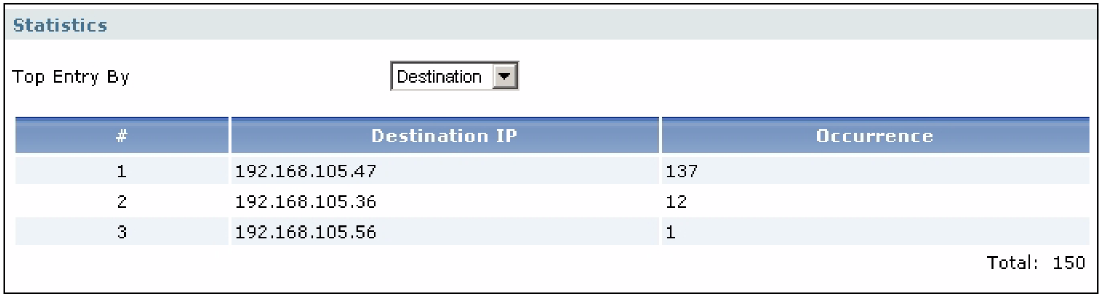


#	Source IP	Occurrence
1	172.23.39.33	150

Total: 150

The statistics display as follows when you display the top entries by destination.

Figure 477 Maintenance > Report > Anti-Virus: Destination



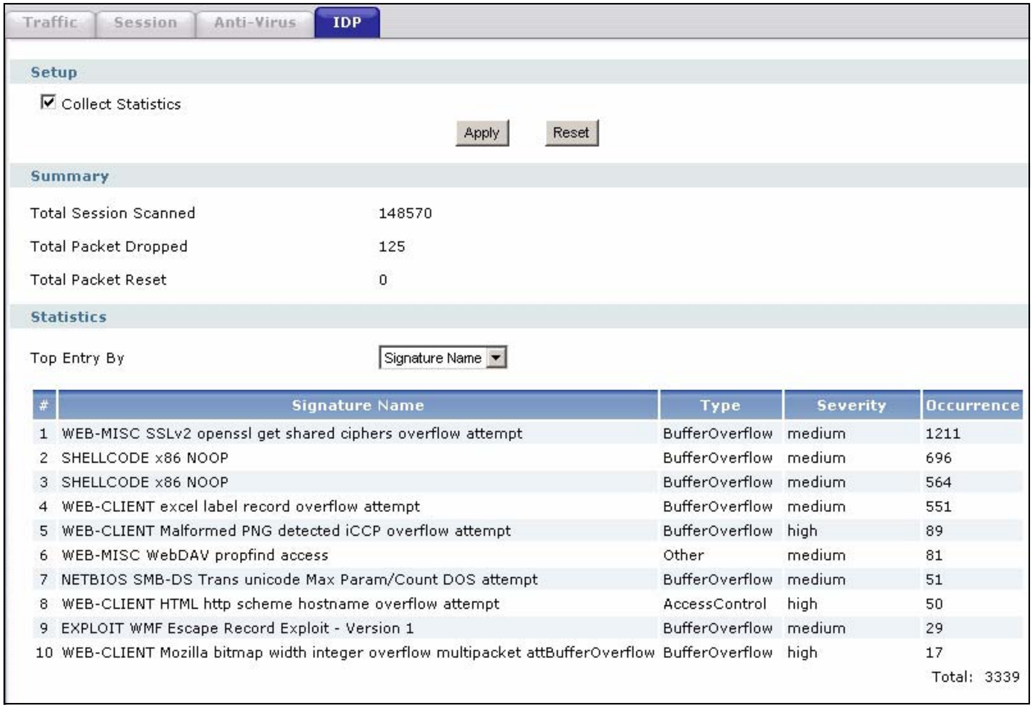
#	Destination IP	Occurrence
1	192.168.105.47	137
2	192.168.105.36	12
3	192.168.105.56	1

Total: 150

47.4 IDP Report Screen

Click **Maintenance** > **Report** > **IDP** to display the following screen. This screen displays IDP (Intrusion Detection and Prevention) statistics.

Figure 478 Maintenance > Report > IDP: Signature Name



☑ Collect Statistics

Total Session Scanned 148570

Total Packet Dropped 125

Total Packet Reset 0

Top Entry By: Signature Name

#	Signature Name	Type	Severity	Occurrence
1	WEB-MISC SSLv2 openssl get shared ciphers overflow attempt	BufferOverflow	medium	1211
2	SHELLCODE x86 NOOP	BufferOverflow	medium	696
3	SHELLCODE x86 NOOP	BufferOverflow	medium	564
4	WEB-CLIENT excel label record overflow attempt	BufferOverflow	medium	551
5	WEB-CLIENT Malformed PNG detected iCCP overflow attempt	BufferOverflow	high	89
6	WEB-MISC WebDAV propfind access	Other	medium	81
7	NETBIOS SMB-DS Trans unicode Max Param/Count DOS attempt	BufferOverflow	medium	51
8	WEB-CLIENT HTML http scheme hostname overflow attempt	AccessControl	high	50
9	EXPLOIT WMF Escape Record Exploit - Version 1	BufferOverflow	medium	29
10	WEB-CLIENT Mozilla bitmap width integer overflow multipacket attBufferOverflow	BufferOverflow	high	17
				Total: 3339

The following table describes the labels in this screen.

Table 229 Maintenance > Report > IDP

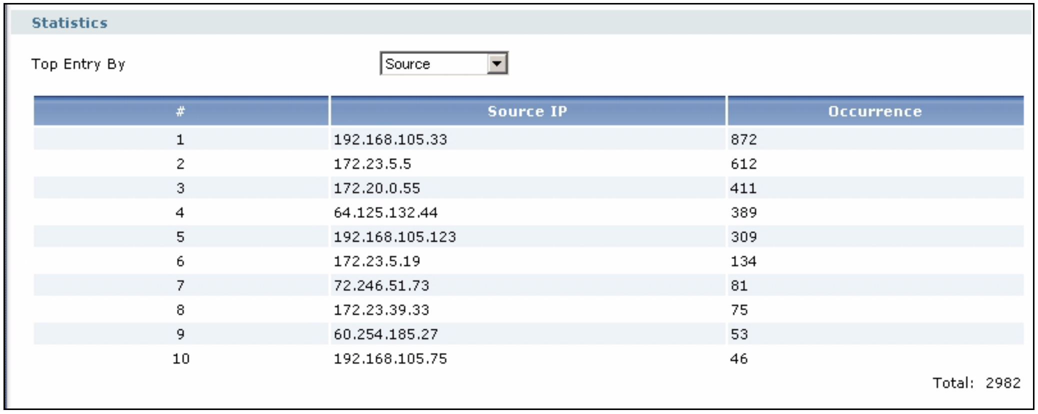
LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the ZyWALL collect IDP statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click the **Flush** button. Collecting starts over and a new collection start time displays.
Total Sessions Scanned	This field displays the number of sessions that the ZyWALL has checked for intrusion characteristics.
Total Sessions Dropped	The ZyWALL can detect and drop malicious sessions from network traffic. This field displays the number of sessions that the ZyWALL has dropped.
Total Sessions Reset	The ZyWALL can detect and reset suspicious network traffic sessions. This field displays the number of sessions that the ZyWALL has reset.
Total Packets Dropped	The ZyWALL can detect and drop malicious packets from network traffic. This field displays the number of packets that the ZyWALL has dropped.
Top Entry By	Use this field to have the following (read-only) table display the top IDP entries by **Signature Name**, **Source** or **Destination**. Select **Signature Name** to list the most common signatures that the ZyWALL has detected. Select **Source** to list the source IP addresses from which the ZyWALL has detected the most intrusion attempts. Select **Destination** to list the most common destination IP addresses for intrusion attempts that the ZyWALL has detected.
#	This field displays the entry's rank in the list of the top entries.
Signature Name	This column displays when you display the entries by **Signature Name**. The signature name identifies a specific intrusion pattern. Click the hyperlink for more detailed information on the intrusion.

Table 229 Maintenance > Report > IDP (continued)

LABEL	DESCRIPTION
Type	This column displays when you display the entries by **Signature Name**. It shows the categories of intrusions. See Table 132 on page 427 for more information.
Severity	This column displays when you display the entries by **Signature Name**. It shows the level of threat that the intrusions may pose. See Table 131 on page 426 for more information.
Source IP	This column displays when you display the entries by **Source.** It shows the source IP address of the intrusion attempts.
Destination IP	This column displays when you display the entries by **Destination.** It shows the destination IP address at which intrusion attempts were targeted.
Occurrences	This field displays how many times the ZyWALL has detected the event described in the entry.
Total	This field displays the sum of the occurrences of the events in the entries.

The statistics display as follows when you display the top entries by source.

Figure 479 Maintenance > Report > IDP: Source



Statistics

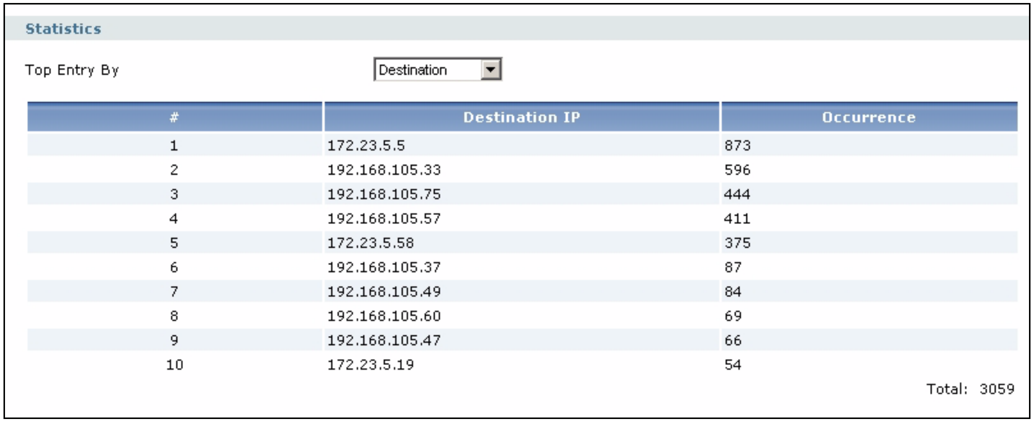
Top Entry By: Source

#	Source IP	Occurrence
1	192.168.105.33	872
2	172.23.5.5	612
3	172.20.0.55	411
4	64.125.132.44	389
5	192.168.105.123	309
6	172.23.5.19	134
7	72.246.51.73	81
8	172.23.39.33	75
9	60.254.185.27	53
10	192.168.105.75	46

Total: 2982

The statistics display as follows when you display the top entries by destination.

Figure 480 Maintenance > Report > IDP: Destination



Statistics

Top Entry By: Destination

#	Destination IP	Occurrence
1	172.23.5.5	873
2	192.168.105.33	596
3	192.168.105.75	444
4	192.168.105.57	411
5	172.23.5.58	375
6	192.168.105.37	87
7	192.168.105.49	84
8	192.168.105.60	69
9	192.168.105.47	66
10	172.23.5.19	54

Total: 3059

48

Diagnostics

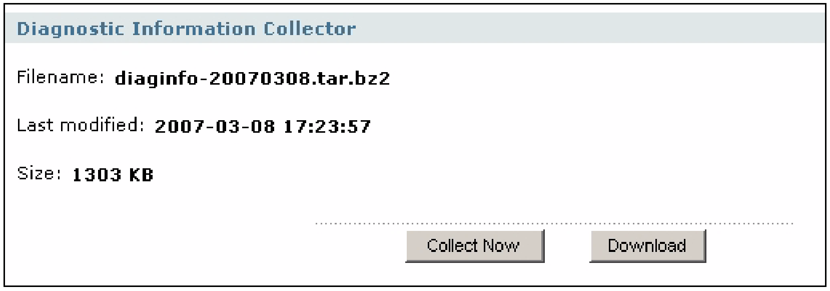
This chapter covers how to use the **Diagnostics** screen.

48.1 Diagnostics

The **Diagnostics** screen provides an easy way for you to generate a file containing the ZyWALL's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

Click **Maintenance** > **Diagnostics** to open the **Diagnostics** screen.

Figure 481 Maintenance > Diagnostics



Diagnostic Information Collector

Filename: diaginfo-20070308.tar.bz2

Last modified: 2007-03-08 17:23:57

Size: 1303 KB

The following table describes the labels in this screen.

Table 230 Maintenance > Diagnostics

LABEL	DESCRIPTION
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Collect Now	Click this to have the ZyWALL create a new diagnostic file.
Download	Click this to save the most recent diagnostic file to a computer.

49

Reboot

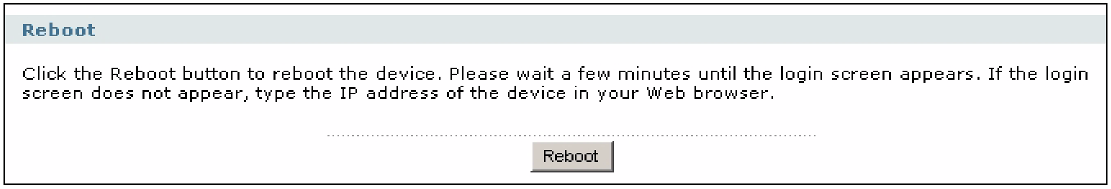
Use this to restart the device (for example, if the device begins behaving erratically). See also Section 1.4 on page 55 for information on different ways to start and stop the ZyWALL.

If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see Section 50.2 on page 652) reset returns the device to its default configuration.

The **Reboot** screen is part of the Web configurator so that remote users can restart the device. To access this screen, click **Maintenance** > **Reboot**.

Figure 482 Maintenance > Reboot



Reboot

Click the Reboot button to reboot the device. Please wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

Click the **Reboot** button to restart the device. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the device.

50

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both ZyXEL IPSec routers and check the settings in each field methodically and slowly. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Section 20.2 on page 296.

- The system log can often help to identify a configuration problem.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (via the IPSec routers).

I cannot set up an L2TP VPN tunnel.

1. Make sure you have configured L2TP correctly on the remote user computers. See Section 26.6 on page 355 for examples.
2. Make sure you configured an appropriate policy route on the ZyWALL.
3. Make sure there is not a firewall or NAT router between the ZyWALL and the remote users.
4. Make sure the remote users are using public IP addresses.

The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

Routing policies define how the ZyWALL forwards packets to their destinations. You must create a policy route for the ZyWALL to route VPN traffic through a VPN tunnel to the remote network.

The VPN wizard automatically creates a corresponding policy route. If you use the **VPN > IPSec VPN** or **VPN > L2TP VPN** screens to set up a VPN tunnel, you need to manually configure a policy route for the VPN tunnel.

? I cannot download the ZyWALL's firmware package.

The ZyWALL's firmware package cannot go through the ZyWALL when you enable the anti-virus **Destroy compressed files that could not be decompressed** option. The ZyWALL classifies the firmware package as not being able to be decompressed and deletes it.

You can upload the firmware package to the ZyWALL with the option enabled, so you only need to clear the **Destroy compressed files that could not be decompressed** option while you download the firmware package. See Section 28.3.1 on page 408 for more on the anti-virus **Destroy compressed files that could not be decompressed** option.

? I changed the LAN IP address and can no longer access the Internet.

If you change the IP address of your LAN interface, make sure you also change the LAN_SUBNET address object.

50.1 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

50.2 Resetting the ZyWALL

If you forget the administrator password(s) or cannot access the ZyWALL by any method, you can reset the ZyWALL to its factory-default settings. Any configuration files or shell scripts that you saved on the ZyWALL should still be available afterwards.

use the following procedure to reset the ZyWALL to its factory-default settings.

This procedure removes the current configuration.

If you want to reboot the device without changing the current configuration, see Chapter 49 on page 649.

1 Make sure the **SYS** LED is on and not blinking.
2 Press the **RESET** button and hold it until the **SYS** LED begins to blink. (This usually takes about five seconds.)
3 Release the **RESET** button, and wait for the ZyWALL to restart.

You should be able to access the ZyWALL using the default settings.

PART VIII

Appendices and Index

Product Specifications (657)
Common Services (703)
Displaying Anti-Virus Alert Messages in Windows (707)
Open Software Announcements (719)
Legal Information (755)
Customer Support (759)
Index (765)

A

Product Specifications

The following specifications are subject to change without notice. See Chapter 2 on page 57 for a general overview of key features.

This table provides basic device specifications.

Table 231 Default Login Information

ATTRIBUTE	SPECIFICATION
Default IP Address (ge1)	192.168.1.1
Default Subnet Mask (ge1)	255.255.255.0 (24 bits)
Default Password	1234

This table provides hardware specifications.

Table 232 Hardware Specifications

FEATURE	SPECIFICATION
Number of MAC addresses	5
Ethernet Interfaces	Number of Ethernet interfaces: 5 All Ethernet interfaces are Gigabit Ethernet, full duplex RJ-45 connectors, auto-negotiation, auto-MDI/MDIX (auto-crossover)
Management interface	RS-232, DB9F connector
AUX port	RS-232, DB9M connector
USB	2, 2.0 plug and play (reserved for future use)
HDD	Slot for an optional 2.5” IDE hard drive (reserved for future use)
Extension Card Slot	Slot for optional hardware accessories (reserved for future use)
Power Requirements	100-240 V AC, 50/60 Hz, 1 A Max
Operating Environment	Temperature: 0 C to 40 C Humidity: 5% to 90% (non-condensing)
Storage Environment	Temperature: -30 C to 60 C Humidity: 5% to 90% (non-condensing)
MTBF	Mean Time Between Failures: 51,611 hours
Dimensions	430.7 (W) x 292.0 (D) x 43.5 (H) mm
Weight	4.7 kg
Rack-mounting	Rack-mountable (rack-mount kit included)

This table gives details about the ZyWALL’s features.

Table 233 Feature Specifications

VERSION # FEATURE	V2.00
# of MAC	5
Flash Size	256
DRAM Size	1024
INTERFACE	
VLAN	32
Virtual (alias)	4 per interface
PPP	12
Bridge	12
ROUTING	
Static Routes	256
Policy Routes	5,000
Sessions	200,000
NAT	
Virtual Servers	up to 1,024
Trigger Port Rules	up to 8 per PR rule
HTTP Redirect	up to interface limit
New Session Rate (sessions per second)	13,000
FIREWALL	
Firewall ACL Rules	5,000
APPLICATION PATROL	
Maximum Rules for Other Protocols	64
Maximum Exception Rules	64
Allowed Ports	NA
Default Ports	8
Address Space Number	NA
USER PROFILES	
Maximum Local Users	1024
Maximum Admin Users	20
Maximum User Groups	256
Maximum Users in One User Group	1024
OBJECTS	
Address Objects	5000
Address Groups	1000
Service Objects	5000

Table 233 Feature Specifications (continued)

VERSION # FEATURE	V2.00
Service Groups	1000
Schedule Objects	512
ISP Accounts	128
Maximum Number of LDAP Groups	16
Maximum Number of LDAP Servers for Each LDAP Group	4
Maximum Number of RADIUS Groups	16
Maximum Number of RADIUS Servers for Each RADIUS Group	4
Maximum Number of Authentication Methods	16
Maximum Number of Zones	16
Maximum Number of Trunks	128
VPN	
Maximum Number of VPN Tunnels	1000
Maximum Number of VPN Concentrators	32
CERTIFICATES	
Certificate Buffer Size	384K
BUILT-IN SERVICES	
A record	1024
NS record	32
MX record	32
Maximum Number of Service Control Entries	32 per service
Maximum Number of DHCP Network Pools	32
Maximum DHCP Host Pool	2048
Maximum Number of DDNS Profiles	10
DHCP Relay	2 per interface
CENTRALIZED LOG	
Log Entries	512
Debug Log Entries	1024
Admin E-mail Addresses	2
Syslog Servers	4
IDP	
Maximum Number of IDP Profiles	8
Custom Signatures	256
CONTENT FILTER	

Table 233 Feature Specifications (continued)

VERSION # FEATURE	V2.00
Maximum Number of Content Filter Policies	64
Maximum Number of Content Filter Profiles	64
Maximum Number of Forbidden Domain Entries	256 per profile
Maximum Number of Trusted Domain Entries	256 per profile
Maximum Number of Keywords that Can Be Blocked	256 per profile
Local Cache Size	8192
Maximum Number of Connections	512
ANTI-VIRUS	
Maximum Number of Concurrent ZIP File Decompression Sessions	100 ZIP files 16 RAR-LZSS or 2 RAR-PPM
SSL VPN	
Maximum SSL VPN Connections	5 without a license 50 with license
OTHERS	
Maximum Number of Device HA VRRP Groups	16
Maximum Number of OSPF Areas	32

The following table, which is not exhaustive, lists standards referenced by ZyWALL features.

Table 234 Standards Referenced by Features

FEATURE	STANDARDS REFERENCED
Interface-Bridge	A subset of the ANSI/IEEE 802.1d standard
Interface	RFCs 2131, 2132, 1541
Interface-PPP	RFCs 1144, 1321, 1332, 1334, 1661, 1662, 2472
Interface-PPTP	RFCs 2637, 3078
Interface-PPPOE	RFC 2516
Interface-VLAN	IEEE 802.1Q
Dynamic Route, Show IP route	RFCs 1058, 2082, 2453, 2328, 3101, 3137
Telnet server	RFCs 1408, 1572
SSH server	RFCs 4250, 4251, 4252, 4253, 4254
Built-in service, DNS server	RFCs 1034, 1035, 1123, 1183, 1535, 1536, 1706, 1712, 1750, 1876, 1982, 1995, 1996, 2136, 2163, 2181, 2230, 2308, 2535, 2536, 2537, 2538, 2539, 2671, 2672, 2673, 2782, 3007, 3090
Built-in service, DHCP server	RFCs 1542, 2131, 2132, 2485, 2489
Built-in service, HTTP server	RFCs 1945, 2616, 2965, 2732, 2295

Table 234 Standards Referenced by Features (continued)

FEATURE	STANDARDS REFERENCED
Built-in service, SNMP agent	RFCs 1067, 1213, 2576, 2578, 2579, 2580, 2741, 2667, 2981, 3371
Login, LDAP support.	RFCs 2251, 2252, 2253, 2254, 2255, 2256, 2589, 2829, 2830
Used by Apache	RFCs 2437, 2246, 2560, 2712, 3268, 3280, 3820, 4132
Built-in service, FTP server	RFCs 959, 2228, 2389, 2865, 2138, 2640
Used by Centralized log	RFC 3164
Login, new PAM module	OSF-RFC 86.0, 1321
Built-in service, NTP client	RFCs 958, 1059, 1119, 1305
Used by SSH service	RFCs 4250, 4251, 4252, 4253, 4254
Used by Time service	RFCs 3339
Used by Telnet service	RFCs 318, 854, 1413
Used by SIP ALG	RFCs 3261, 3264
DHCP relay	RFC 1541
ZySH	W3C XML standard
ARP	RFC 826
IP/IPv4	RFC 791
TCP	RFC 793

B

Log Descriptions

This appendix provides descriptions of example log messages.

Table 235 Content Filter Logs

LOG MESSAGE	DESCRIPTION
`Content filter has been enabled`	An administrator turned the content filter on.
`Content filter has been disabled`	An administrator turned the content filter off.

Table 236 Forward Web Site Logs

LOG MESSAGE	DESCRIPTION
`%s: Trusted Web site`	The device allowed access to a web site in a trusted domain. %s: website host
`%s`	The device allowed access to a web site. The content filtering service is registered and activated or the service is not activated in a profile, this is a web site that is not blocked according to a profile and the default policy is not set to block. %s: website host
`%s: Service is not registered`	The device allowed access to a web site. The content filtering service is unregistered and the default policy is not set to block. %s: website host

Table 237 Blocked Web Site Logs

LOG MESSAGE	DESCRIPTION
`%s :%s`	The rating server responded that the web site is in a specified category and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
`%s: Unrated`	The rating server responded that the web site cannot be categorized and access was blocked according to a content filter profile. %s: website host

Table 237 Blocked Web Site Logs (continued)

LOG MESSAGE	DESCRIPTION
`%s: Service is unavailable`	Content filter rating service is temporarily unavailable and access to the web site was blocked due to: 1. Can't resolve rating server IP (No DNS) 2. Invalid service license 4. Rating service is restarting 5. Can’t connect to rating server 6. Query failed 7. Query timeout 8. Too many queries 9. Unknown reason %s: website host
`%s: %s(cache hit)`	The web site's category exists in the device’s local cache and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
`%s: Not in trusted web list`	The web site is not a trusted host/domain, and the device blocks all traffic except for trusted web sites. %s: website host
`%s: Contains ActiveX`	The web site contains ActiveX and access was blocked according to a profile. %s: website host
`%s: Contains Java applet`	The web site contains Java applet and access was blocked according to a profile. %s: website host
`%s: Contains cookie`	The web site contains a cookie and access was blocked according to a profile. %s: website host
`%s: Proxy mode is detected`	The system detected a proxy connection and blocked access according to a profile. %s: website host
`%s: Forbidden Web site`	The web site is in forbidden web site list. %s: website host
`%s: Keyword blocking`	The web content matched a user defined keyword. %s: website host
`%s: Blocking by default policy`	No content filter policy is applied and access was blocked since the default action is block. %s: website host

Table 238 User Logs

LOG MESSAGE	DESCRIPTION
`%s %s has logged in from %s`	The specified user signed in. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
`%s %s has logged out from %s`	The specified user signed out. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
`%s %s from %s has been logged out (re-auth timeout)`	The specified user was signed out by the device due to a re-authentication timeout. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
`%s %s from %s has been logged out (lease timeout)`	The specified user was signed out by the device due to a lease timeout. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
`%s %s from %s has been logged out (idle timeout)`	The specified user was signed out by the device due to an idle timeout. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
`Console is put into lockout`	Too many failed login attempts were made on the console port so the device is blocking login attempts on the console port.
`Address %u.%u.%u.%u is put into lockout`	Too many failed login attempts were made from an IP address so the device is blocking login attempts from that IP address. %u.%u.%u.%u: the source address of the user’s login attempt
`Login attempt is made on a lockout address from %s`	A login attempt came from an IP address that the device has locked out. %u.%u.%u.%u: the source address of the user’s login attempt
`Failed %s login attempt (reach the maximum number of user)`	The device blocked a login because the maximum login capacity has already been reached. %s: service name
`Failed %s login attempt (reach the maximum number of simultaneous logon)`	The device blocked a login because the maximum simultaneous login capacity for the administrator or access account has already been reached. %s: service name

Table 239 myZyXEL.com Logs

LOG MESSAGE	DESCRIPTION
`Send registration message to MyZyXEL.com server has failed.`	The device was not able to send a registration message to MyZyXEL.com.
`Get server response has failed.`	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
`Timeout for get server response.`	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
`User has existed.`	The user name already exists in MyZyXEL.com's database. So the user can't use it for device registration and needs to specify another one.
`User does not exist.`	The user name does not yet exist in MyZyXEL.com's database. So the user can use it for device registration.
`Internal server error.`	MyZyXEL.com's database had an error when checking the user name.
`Device registration has failed:%s.`	Device registration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by the myZyXEL.com server
`Device registration has succeeded.`	The device registered successfully with the myZyXEL.com server.
`Registration has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`%s:Trial service activation has failed:%s.`	Trail service activation failed for the specified service, an error message returned by the MyZyXEL.com server will be appended to this log. 1st %s: service name 2nd %s: error message returned by the myZyXEL.com server
`%s:Trial service activation has succeeded.`	Trail service was activated successfully for the specified service. %s: service name
`Trial service activation has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`Standard service activation has failed:%s.`	Standard service activation failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by the myZyXEL.com server
`Standard service activation has succeeded.`	Standard service activation has succeeded.
`Standard service activation has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`Service expiration check has failed:%s.`	The service expiration day check failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by myZyXEL.com server

Table 239 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Service expiration check has succeeded.`	The service expiration day check was successful.
`Service expiration check has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`Server setting error.`	The device could not retrieve the myZyXEL.com server's IP address or FQDN from local.
`Resolve server IP has failed.`	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
`Verify server's certificate has failed.`	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate.
`Connect to MyZyXEL.com server has failed.`	The device could not connect to the MyZyXEL.com server.
`Do account check.`	The device started to check whether or not the user name in MyZyXEL.com's database.
`Do device register.`	The device started device registration.
`Do trial service activation.`	The device started trail service activation.
`Do standard service activation.`	The device started standard service activation.
`Do expiration check.`	The device started the service expiration day check.
`Build query message has failed.`	Some information was missing in the packets that the device sent to the MyZyXEL.com server.
`Parse receive message has failed.`	The device cannot parse the response returned by the MyZyXEL.com server. Maybe some required fields are missing.
`Resolve server IP has failed. Update stop.`	The update has stopped because the device couldn't resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
`Verify server's certificate has failed. Update stop.`	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate. The update has stopped.
`Send download request to update server has failed.`	The device's attempt to send a download message to the update server failed.
`Get server response has failed.`	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
`Timeout for get server response.`	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
`Send update request to update server has failed.`	The device could not send an update message to the update server.
`Update has failed. Because of lack must fields.`	The device received an incomplete response from the update server and it caused a parsing error for the device.

Table 239 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Update server is busy now. File download after %d seconds.`	The update server was busy so the device will wait for the specified number of seconds and send the download request to the update server again.
`Device has latest file. No need to update.`	The device already has the latest version of the file so no update is needed.
`Device has latest signature file; no need to update`	The device already has the latest version of the signature file so no update is needed.
`Connect to update server has failed.`	The device cannot connect to the update server.
`Wrong format for packets received.`	The device cannot parse the response returned by the server. Maybe some required fields are missing.
`Server setting error. Update stop.`	The device could not resolve the update server's FQDN to an IP address through gethostbyname(). The update process stopped.
`Build query message failed.`	Some information was missing in the packets that the device sent to the server.
`Starting signature update.`	The device started an IDP signature update.
`Signature download has succeeded.`	The device successfully downloaded a signature file.
`Signature update has succeeded.`	The device successfully downloaded and applied an IDP signature file.
`Signature update has failed:%s.`	The signature update signature failed, an error message returned by the update server will be appended to this log. %s: error message returned by update server
`Signature download has failed.`	The device still can't download the IDP signature after 3 retries.
`Signature update has failed. Do %d retry.`	The IDP signature update failed, so the device will process 3 retries. %d: retry times (1~3)
`Resolve server IP has failed.`	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
`Connect to MyZyXEL.com server has failed.`	The device could not connect to the MyZyXEL.com server.
`Build query message has failed.`	Some information was missing in the packets that the device sent to the server.
`Verify server's certificate has failed.`	The device could not process an HTTPS connection because it could not verify the server's certificate.
`Get server response has failed.`	The device sent packets to the server, but did not receive a response. The root cause may be that the connection is abnormal.
`Expiration daily-check has failed:%s.`	The daily check for service expiration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by myZyXEL.com server

Table 239 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Do expiration daily-check has failed. Because of lack must fields.`	The device received an incomplete response to the daily service expiration check and the packets caused a parsing error for the device.
`Server setting error.`	The device could not retrieve the server's IP address or FQDN from local.
`Do expiration daily-check has failed.`	The daily check for service expiration failed.
`Do expiration daily-check has succeeded.`	The daily check for service expiration was successful.
`Expiration daily-check will trigger PPP interface. Do self-check.`	Before the device sends an expiration day check packet, it needs to check whether or not it will trigger a PPP connection.
`System bootup. Do exipration daily-check.`	The device processes a service expiration day check immediately after it starts up.
`After register. Do expiration daily-check immediately.`	The device processes a service expiration day check immediately after device registration.
`Time is up. Do exipration daily-check.`	The processes a service expiration day check every 24 hrs.
`Read MyZyXEL.com storage has failed.`	Read data from EEPROM has failed.
`Open /proc/MRD has failed.`	This error message is shown when getting MAC address.
`IDP service has expired.`	The IDP service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device’s own count.
`Content-Filter service has expired.`	The content filtering service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device’s own count.
`Unknown TLS/SSL version: %d.`	The device only supports SSLv3 protocol. %d: SSL version assigned by client.
`Load trusted root certificates has failed.`	The device needs to load the trusted root certificate before the device can verify a server's certificate. This log displays if the device failed to load it.
`Certificate has expired.`	Verification of a server’s certificate failed because it has expired.
`Self signed certificate.`	Verification of a server’s certificate failed because it is self-signed.
`Self signed certificate in certificate chain.`	Verification of a server’s certificate failed because there is a self-signed certificate in the server’s certificate chain.
`Verify peer certificates has succeeded.`	The device verified a server’s certificate while processing an HTTPS connection.

Table 239 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Certification verification failed: Depth: %d, Error Number(%d):%s.`	Verification of a server's certificate failed while processing an HTTPS connection. This log identifies the reason for the failure. 1st %d: certificate chain level 2nd %d: error number %s: error message
`Certificate issuer name:%s.`	Verification of the specified certificate failed because the device could not get the certificate's issuer name. %s is the certificate name.
`The wrong format for HTTP header.`	The header format of a packet returned by a server is wrong.
`Timeout for get server response.`	After the device sent packets to a server, the device did not receive any response from the server. The root cause may be a network delay issue.
`Download file size is wrong.`	The file size downloaded for AS is not identical with content-length
`Parse HTTP header has failed.`	Device can't parse the HTTP header in a response returned by a server. Maybe some HTTP headers are missing.

Table 240 IDP Logs

LOG MESSAGE	DESCRIPTION
`System internal error. Detect IDP engine status failed.`	System internal error. Get IDP engine activation flag failed.
`System internal error. Enable IDP failed.`	Enable IDP engine activation flag failed.
`System internal error.Disable IDP failed.`	Disable IDP engine activation flag failed.
`Enable IDP succeeded.`	Enable IDP engine succeeded.
`Disable IDP succeeded.`	Disable IDP engine succeeded.
`Enable IDP engine failed.`	Insert IDP engine failed.
`Disable IDP engine failed.`	Remove IDP engine failed.
`Enable IDP engine succeeded.`	Insert IDP engine succeeded.
`Disable IDP engine succeeded.`	Remove IDP engine succeeded.
`IDP service is not registered. Packet Inspection feature will not be activated.`	IDP service is not registered. IDP service packet inspection feature and signature update will both be deactivated.
`IDP service trial license is expired. Packet Inspection feature will not be activated.`	IDP service trial license is expired. IDP service packet inspection feature and signature update will both be deactivated.

Table 240 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
IDP service standard license is expired. Update signature failed.	IDP service standard license is expired. IDP signature cannot update.
IDP service standard license is not registered. Update signature failed.	IDP service standard license is not registered. IDP signature cannot update.
IDP service trial license is expired. Update signature failed.	IDP service trial license is expired. IDP signature cannot update.
IDP service trial license is not registered. Update signature failed.	IDP service trial license is expired. IDP signature cannot update.
Custom signature add error: sid *<sid>*, *<error_message>.*	Custom signature adding failed. Error sid and message will be shown.
Custom signature import error: line *<line>*, sid *<sid>*, *<error_message>.*	Custom signature importing failed. Error line number of file, sid and message will be shown
Custom signature replace error: line *<line>*, sid *<sid>*, *<error_message>.*	Custom signature replacing failed. Error line number of file, sid and message will be shown
Custom signature edit error: sid *<sid>*, *<error_message>.*	Custom signature editing failed. Error sid and message will be shown.
Custom signature more than *<num>*. Replacement custom signature number is *<num>*.	Custom signature replacement failed. Display maximum rule number and replacement rule number.
Custom signature more than *<num>*. Remaining custom signature number is *<num*. Adding custom signature number is *<num>*.	Custom signature adding failed. Display maximum rule number, remaining rule number and adding rule number.
Get custom signature number error.	Get custom rule number failed.
Add custom signature error: signature *<sid>* is over length.	Custom signature adding failed. Rule content length is too long.
Edit custom signature error: signature *<sid>* is over length.	Custom signature editing failed. Rule content length is too long.

Table 240 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
`IDP off-line update failed. File damaged.`	IDP signature off-line update failed. Signature file maybe corrupt.
`IDP signature update failed. File crashed.`	IDP signature update failed. Decrypt signature file failed.
`IDP signature update failed. File damaged.`	IDP signature update failed. Decompress signature file failed.
`IDP signature update failed. File update failed.`	IDP signature update failed. Update signature file filed.
`IDP signature update failed. Can not update last update time.`	IDP signature update failed. Update last update time failed.
`IDP signature update failed. Can not update synchronized file.`	IDP signature update failed. Rebuild IDP DHA synchronized file failed.
`IDP signature update successful. Signature version:` *`<version>.`*	IDP signature update successful.
`System internal error. Create IDP debug directory failed`	System internal error. Create IDP debug directory failed.
`System internal error. Create IDP statistics entry failed.`	System internal error. Create IDP statistics entry failed.
`System internal error. Out of memory. IDP activation unchanged.`	System internal error. System is out of memory. IDP activation unchanged.
`System internal error. Create IDP proc failed. IDP activation failed.`	System internal error. Create IDP proc failed. IDP activation failed.
`[type=`*`<type>`*`]` *`<message>`*`, Action:` *`<action>`*`, Severity:` *`<severity>`*	IDP triggered event log. <*type*> = {sig(<*id*>) | scan-detection(<*attack*>) | flood-detection(<*attack*>) | http-inspection(<*attack*>) | tcp-decoder(<*attack*>) | udp-decoder(<*attack*>) | icmp-decoder(<*attack*>) }, <*attack*> = attack type. <severity> = {very low | low | medium | high | severe}
`Program DFA failed.`	IDP program DFA to hardware search engine failed.
`IDP sigature update failed. Fail to create temporary directory`	IDP signature update failed. Create /tmp/sig directory failed
`IDP sigature update failed. Fail to extract temporary file.`	IDP signature update failed. Extract signature package to /tmp/sig failed.
`IDP signature update failed. Invalid IDP config file.`	IDP signature update failed. Sig_check_update check failed.

Table 240 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
`IDP signature update failed. Invalid signature content.`	IDP signature update failed. Sigquery check signature content failed.
`System internal error. Create IDP traffic anomaly entry failed.`	System internal error. Create IDP traffic anomaly entry failed.
`Query signature version failed.`	Unable to get signature version from new signature package download from update server
`Can not get signature version.`	Unable to get signature version from new signature package download from update server

Table 241 Application Patrol Logs

LOG MESSAGE	DESCRIPTION
`System fatal error: 60005001.`	Application patrol zysh initialization failed. Protocol file import error.
`System fatal error: 60005002.`	Application patrol zysh initialization failed. Shared memory failed.
`System fatal error: 60005017.`	Application patrol zyio failed. Fail to do zyio operation.
`System fatal error: 60005018.`	Application patrol kernel error. Fail to communicate with kernel module.
`System fatal error: 60005019.`	Application patrol configuration group error. Fail to retrieve use group from use object.
`System fatal error: 60006004.`	Application patrol daemon (process) shared memory key generating fail.
`System fatal error: 60006021.`	Error generating application patrol semaphore key.
`System fatal error: 60006031.`	Warning application patrol resources ran out! New configuration of affected rule [%s:%d] is discarded.
`System fatal error: 60018001.`	Application patrol daemon (process) out of share memory address pool.
`System fatal error: 60018002.`	Application patrol daemon (process) ran out of pre-allocated share memory.
`System fatal error: 60018003.`	Application patrol daemon (process) failed to lock shared memory.
`System fatal error: 60018004.`	Application patrol daemon (process) failed to unlock shared memory.
`System fatal error: 60018005.`	Error generating application patrol semaphore key.
`System fatal error: 60018006.`	Application patrol daemon (process) fails to create share memory.
`System fatal error: 60018007.`	Error opening /dev/l7_action device.
`System fatal error: 60018008.`	Error when do ioctl L7_ACTION_IOCTL_ADDR_USAGE.

Table 241 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
`System fatal error: 60018009.`	Error when do ioctl L7_ACTION_IOCTL_ADDR_USAGE.
`System fatal error: 60018010.`	Error when do ioctl L7_ACTION_IOCTL_PROTO_ADDR_NUMS.
`System fatal error: 60018011.`	Fail to user lib user_profile to retrieve current login user.
`System fatal error: 60018012.`	Fail to user lib user_profile to retrieve current login user.
`System fatal error: 60018013.`	Fail to user lib user_profile to retrieve current login user.
`System fatal error: 60018014.`	Fail to user lib user_profile to retrieve current login user.
`System fatal error: 60018015.`	Fail to retrieve user event from uamd.
`System fatal error: 60018016.`	Application patrol daemon (process) shared memory generate failed.
`System fatal error: 60018017.`	Fail to get share memory.
`System fatal error: 60018018.`	Fail to get attach memory.
`System fatal error: 60018019.`	Application patrol daemon receive restart signal.
`System fatal error: 60018020.`	Application patrol daemon signal handler failed.
`System fatal error: 60018021.`	Application patrol daemon initialization failed.
`System fatal error: 60018022.`	Application patrol daemon startup failed.
`System fatal error: 60018023.`	Application patrol daemon stop.
`Activate App. Patrol has succeeded.`	Activate application patrol has succeeded.
`No '%s' protocol.`	The protocol %s does not exist. %s: Protocol Name
`Service %s has been activated.`	Protocol %s is active. %s: Protocol Name
`Deactivate App Patrol has succeeded.`	Deactivation of application patrol has succeeded.
`Initialize App. Patrol has succeeded.`	Initialization application patrol has succeeded.

Table 241 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
`App Patrol Name=%s Type=%s %s=%d Protocol=%s Action=%s`	Packets logging. 1st %s: Protocol Name, 2nd %s: Category Name, 3rd %s: Default Rule or Exception Rule, 1st %d: Rule Index, 4th %s: TCP or UDP, 5th %s: Action.
`App Patrol resources ran out. User %s is unrestricted by rule [ %s:%d ].  1st %s: User Name, 2nd %s: Protocol Name, 1% %d: Rule Index`	The application patrol daemon (process) resource pool is full, current login user %s is unrestricted by rule %d of protocol %s. 1st %s: User Name, 1st %d: Rule Index, 2nd %s: Protocol Name.

Table 242 IKE Logs

LOG MESSAGE	DESCRIPTION
`%s:%s has not announced DPD capability`	%s:%s is the peer IP:Port. Peer has not announced capability.
`[COOKIE] Invalid cookie, no sa found`	Cannot find SA according to the cookie.
`[DPD] No response from "%s:%s using existing Phase-1 SA in %u seconds. Trying with Phase-1 rekey.`	%s:%s is the peer IP:Port. %u is the retry time. Dead Peer Detection (DPD) detected no response from peer.
`[HASH] : Tunnel [%s] Phase 1 hash mismatch`	`%s` is the tunnel name. When negotiating Phase-1, the exchange hash did not match.
`[HASH] : Tunnel [%s] Phase 2 hash mismatch"`	`%s` is the tunnel name. When negotiating Phase-2, the calculated quick mode authentication hash did not match.
`[ID] : Invalid ID information`	ID payload is not valid (in Phase-1 is local/peer ID, in Phase-2 is local/remote policy).
`[ID] : Tunnel [%s] Local IP mismatch`	`%s` is the tunnel name. When negotiating Phase-1, the local tunnel IP did not match the My IP in VPN gateway.
`[ID] : Tunnel [%s] My IP mismatch`	`%s` is the tunnel name. When negotiating Phase-1 and selecting matched proposal, My IP Address could not be resolved.
`[ID] : Tunnel [%s] Phase 1 ID mismatch`	`%s` is the tunnel name. When negotiating Phase-1, the peer ID did not match.
`[ID] : Tunnel [%s] Phase 2 Local ID mismatch`	`%s` is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.
`[ID] : Tunnel [%s] Phase 2 Remote ID mismatch`	`%s` is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.
`[ID] : Tunnel [%s] Remote IP mismatch`	%s is the tunnel name. When negotiating Phase-1, the peer tunnel IP did not match the secure gateway address in VPN gateway.
`[SA] : Malformed IPSec SA proposal`	When selecting a matched proposal, some protocol was given more than once.
`[SA] : No proposal chosen`	When selecting a matched proposal in phase-1 or phase-2, so proposal was selected.

Table 242 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`[SA] : Tunnel [%s] Phase 1 authentication algorithm mismatch`	%s is the tunnel name. When negotiating Phase-1, the authentication algorithm did not match.
`[SA] : Tunnel [%s] Phase 1 authentication method mismatch`	%s is the tunnel name. When negotiating Phase-1, the authentication method did not match.
`[SA] : Tunnel [%s] Phase 1 encryption algorithm mismatch`	%s is the tunnel name. When negotiating Phase-1, the encryption algorithm did not match.
`[SA] : Tunnel [%s] Phase 1 invalid protocol`	%s is the tunnel name. When negotiating Phase-1, the packet was not a ISKAMP packet in the protocol field.
`[SA] : Tunnel [%s] Phase 1 invalid transform`	%s is the tunnel name. When negotiating Phase-1, the transform ID was invalid.
`[SA] : Tunnel [%s] Phase 1 key group mismatch`	%s is the tunnel name. When negotiating Phase-1, the DH group of the attribute list `attrs' did not match the security policy.
`[SA] : Tunnel [%s] Phase 1 negotiation mode mismatch`	%s is the tunnel name. When negotiating Phase-1, the negotiation mode did not match.
`[SA] : Tunnel [%s] Phase 2 authentication algorithm mismatch`	%s is the tunnel name. When negotiating Phase-2, the authentication algorithm did not match.
`[SA] : Tunnel [%s] Phase 2 encapsulation mismatch`	%s is the tunnel name. When negotiating Phase-2, the encapsulation did not match.
`[SA] : Tunnel [%s] Phase 2 encryption algorithm mismatch`	%s is the tunnel name. When negotiating Phase-2, the encryption algorithm did not match.
`[SA] : Tunnel [%s] Phase 2 pfs mismatch`	%s is the tunnel name. When negotiating Phase-2, the PFS specified did not match.
`[SA] : Tunnel [%s] Phase 2 pfs unsupported: %d`	%s is the tunnel name. When negotiating Phase-2, this device does not support the PFS specified.
`[SA] : Tunnel [%s] Phase 2 SA encapsulation mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA encapsulation did not match.
`[SA] : Tunnel [%s] Phase 2 SA protocol mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA protocol did not match.
`[SA] : Tunnel [%s] SA sequence size mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA sequence size did not match.
`[XCHG] exchange type is not IP, AGGR, or INFO`	This device is the responder and this is the initiator's first packet, but exchange type is not IP, AGGR, or INFO and the packet is ignored.

Table 242 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Cannot resolve My IP Addr %s for Tunnel [%s]`	1st %s is my ip address. 2nd %s is the tunnel name. When selecting a matched proposal in phase-1, the engine could not get My-IP address.
`Cannot resolve Secure Gateway Addr %s for Tunnel [%s]`	1st %s is my ip address. 2nd %s is the tunnel name; When selecting a matched proposal in phase-1, the engine could not get the correct secure gateway address.
`Could not dial dynamic tunnel "%s"`	%s is the tunnel name. The tunnel is a dynamic tunnel and the device cannot dial it.
`Could not dial incomplete tunnel "%s"`	%s is the tunnel name. The tunnel setting is not complete.
`Could not dial manual key tunnel "%s"`	%s is the tunnel name. The manual key tunnel cannot be dialed.
`DPD response with invalid ID`	When receiving a DPD response with invalid ID ignored.
`DPD response with no active request`	When receiving a DPD response with no active query.
`IKE Packet Retransmit`	When retransmitting the IKE packets.
`Phase 1 IKE SA process done`	When Phase 1 negotiation is complete.
`Recv Main Mode request from [%s]`	%s is the remote name; When receiving a request to enter Main mode.
`Recv Aggressive Mode request from [%s]`	%s is the remote name; When receiving a request to enter Aggressive mode.
`Recv DPD request from "%s:%s"`	%s:%s is peer IP:Port. The device received a Dead Peer Detection request.
`Recv DPD response from "%s:%s"`	%s:%s is peer IP:Port. The device received a Dead Peer Detection response.
`Recv:[SA]%s[KE]%s[ID]%s[CERT]%s[CR]%s[HASH]%s[SIG]%s[NONCE]%s[DEL]%s[VID]%s[ATTR]%s`	This is a combined message for incoming IKE packets.
`Send Main Mode request to [%s]`	%s is the remote name. The device sent a request to enter Main Mode.
`Send Aggressive Mode request to [%s]`	%s is the remote name. The device sent a request to enter Aggressive Mode.
`Send DPD request to "%s:%s"`	%s:%s is peer IP:Port. The device sent a Dead Peer Detection request to the peer.
`Send DPD response to "%s:%s"`	%s:%s is peer IP:Port. The device sent a DPD response sent to the peer.
`Send:[ID]%s[SA]%s[KE]%s[ID]%s[CERT]%s[CR]%s[HASH]%s[SIG]%s[NONCE]%s[DEL]%s[VID]%s[ATTR]%s[`	This is a combined message for outgoing IKE packets.
`Start Phase 2: Quick Mode`	Indicates the beginning of phase 2 using quick mode.

Table 242 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`The cookie pair is : 0x%08x%08x / 0x%08x%08x`	Indicates the initiator/responder cookie pair.
`The IPSec tunnel "%s" is already established`	%s is the tunnel name. When dialing a tunnel, the tunnel is already dialed.
`Tunnel [%s] built successfully`	%s is the tunnel name. The phase-2 tunnel negotiation is complete.
`Tunnel [%s] Phase 1 pre-shared key mismatch`	%s is the tunnel name. When negotiating phase-1, the pre-shared key did not match.
`Tunnel [%s] Recving IKE request`	%s is the tunnel name. The device received an IKE request.
`Tunnel [%s] Sending IKE request`	%s is the tunnel name. The device sent an IKE request.
`Tunnel [%s] IKE Negotiation is in process`	%s is the tunnel name. When IKE request is already sent but still attempting to dial a tunnel.
`VPN gateway %s was disabled`	%s is the gateway name. An administrator disabled the VPN gateway.
`VPN gateway %s was enabled`	%s is the gateway name. An administrator enabled the VPN gateway.
`XAUTH fail! My name: %s`	%s is the my xauth name. This indicates that my name is invalid.
`XAUTH fail! Remote user: %s`	%s is the remote xauth name. This indicates that a remote user's name is invalid.
`XAUTH succeed! My name: %s`	%s is the my xauth name. This indicates that my name is valid.
`XAUTH succeed! Remote user: %s`	%s is the remote xauth name. This indicate that a remote user's name is valid
`Dynamic Tunnel [%s:%s:0x%x:%s] built successfully`	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
`Dynamic Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully`	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
`Tunnel [%s:%s:0x%x:%s] built successfully`	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
`Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully`	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
`Tunnel [%s:%s]  Phase 1 pre-shared key mismatch`	The variables represent the phase 1 name and tunnel name. When negotiating phase-1, the pre-shared keys did not match.
`Tunnel [%s:%s] Recving IKE request`	The variables represent the phase 1 name and tunnel name. The device received an IKE request.

Table 242 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Tunnel [%s:%s] Sending IKE request`	The variables represent the phase 1 name and tunnel name. The device sent an IKE request.
`Tunnel [%s:0x%x] is disconnected`	The variables represent the tunnel name and the SPI of a tunnel that was disconnected.
`Tunnel [%s] rekeyed successfully`	%s is the tunnel name. The tunnel was rekeyed successfully.

Table 243 IPSec Logs

LOG MESSAGE	DESCRIPTION
`Corrupt packet, Inbound transform operation fail`	The device received corrupt IPsec packets and could not process them.
`Encapsulated packet too big with length`	An outgoing packet needed to be transformed but was longer than 65535.
`Get inbound transform fail`	When performing inbound processing for incoming IPSEC packets and ICMPs related to them, the engine cannot obtain the transform context.
`Get outbound transform fail`	When outgoing packet need to be transformed, the engine cannot obtain the transform context.
`Inbound transform operation fail`	After encryption or hardware accelerated processing, HWAccel dropped packet (resource shortage, corrupt packet, invalid MAC, and so on).
`Outbound transform operation fail`	After encryption or hardware accelerated processing, Hwaccel dropped packet (e.g., resource overflow, corrupt packet, and so on).
`Packet too big with Fragment Off`	An outgoing packet needed to be transformed, but the fragment flag was off and the packet was too big.
`SPI:0x%x SEQ:0x%x Execute transform step fail, ret=%d`	The variables represent the SPI, sequence number and the error number. When trying to perform transforming, the engine returned an error.
`SPI:0x%x SEQ:0x%x No rule found, Dropping packet`	The variables represent the SPI and the sequence number. The packet did not match the tunnel policy and was dropped.
`SPI:0x%x SEQ:0x%x Packet Anti-Replay detected`	The variables represent the SPI and the sequence number. The device received a packet again (that it had already received).
`VPN connection %s was disabled.`	`%s` is the VPN connection name. An administrator disabled the VPN connection.
`VPN connection %s was enabled.`	`%s` is the VPN connection name. An administrator enabled the VPN connection.

Table 244 Firewall Logs

LOG MESSAGE	DESCRIPTION
`priority:%lu, from %s to %s, service %s, %s`	1st variable is the global index of rule, 2nd is the from zone, 3rd is the to zone, 4th is the service name, 5th is ACCEPT/DROP/ REJECT.
`%s:%d: in %s():`	Firewall is dead, trace to %s is which file, %d is which line, %s is which function
`Firewall has been %s.`	%s is enabled/disabled
`Firewall rule %d has been moved to %d.`	1st %d is the old global index of rule, 2nd %d is the new global index of rule
`Firewall rule %d has been deleted.`	%d is the global index of rule
`Firewall rules have been flushed.`	Firewall rules were flushed
`Firewall rule %d was %s.`	%d is the global index of rule, %s is appended/inserted/modified
`Firewall %s %s rule %d was %s.`	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule 3rd %s is appended/inserted/modified
`Firewall %s %s rule %d has been moved to %d.`	1st %s is from zone, 2nd %s is to zone, 1st %d is the old index of the rule 2nd %d is the new index of the rule
`Firewall %s %s rule %d has been deleted.`	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule
`Firewall %s %s rules have been flushed.`	1st %s is from zone, 2nd %s is to zone
`abnormal TCP flag attack detected`	Abnormal TCP flag attack detected
`invalid state detected`	Invalid state detected
`The Asymmetrical Route has been enabled.`	Asymmetrical route has been turned on.
`The Asymmetrical Route has been disabled.`	Asymmetrical Route has been turned off.

Table 245 Sessions Limit Logs

LOG MESSAGE	DESCRIPTION
`Maximum sessions per host (%d) was exceeded.`	%d is maximum sessions per host.

Table 246 Policy Route Logs

LOG MESSAGE	DESCRIPTION
`Cann't open bwm_entries`	Policy routing can't activate BWM feature.
`Cann't open link_down`	Policy routing can't detect link up/down status.

Table 246 Policy Route Logs (continued)

LOG MESSAGE	DESCRIPTION
`Cannot get handle from UAM, user-aware PR is disabled`	User-aware policy routing is disabled due to some reason.
`mblock: allocate memory failed!`	Allocating policy routing rule fails: insufficient memory.
`pt: allocate memory failed!`	Allocating policy routing rule fails: insufficient memory.
`To send message to policy route daemon failed!`	Failed to send control message to policy routing manager.
`The policy route %d allocates memory fail!`	Allocating policy routing rule fails: insufficient memory. %d: the policy route rule number
`The policy route %d uses empty user group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty source address group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty destination address group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty service group`	Use an empty object group. %d: the policy route rule number
`Policy-route rule %d was inserted.`	Rules is inserted into system. %d: the policy route rule number
`Policy-route rule %d was appended.`	Rules is appended into system. %d: the policy route rule number
`Policy-route rule %d was modified.`	Rule is modified. %d: the policy route rule number
`Policy-route rule %d was moved to %d.`	Rule is moved. 1st %d: the original policy route rule number 2nd %d: the new policy route rule number
`Policy-route rule %d was deleted.`	Rule is deleted. %d: the policy route rule number
`Policy-route rules were flushed.`	Policy routing rules are cleared.

Table 247 Built-in Services Logs

LOG MESSAGE	DESCRIPTION
`User on %u.%u.%u.%u has been denied access from %s`	HTTP/HTTPS/TELNET/SSH/FTP/SNMP access to the device was denied. %u.%u.%u.%u is IP address %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET
`HTTPS certificate:%s does not exist. HTTPS service will not work.`	An administrator assigned a nonexistent certificate to HTTPS. %s is certificate name assigned by user
`HTTPS port has been changed to port %s.`	An administrator changed the port number for HTTPS. %s is port number
`HTTPS port has been changed to default port.`	An administrator changed the port number for HTTPS back to the default (443).
`HTTP port has changed to port %s.`	An administrator changed the port number for HTTP. %s is port number assigned by user
`HTTP port has changed to default port.`	An administrator changed the port number for HTTP back to the default (80).
`SSH port has been changed to port %s.`	An administrator changed the port number for SSH. %s is port number assigned by user
`SSH port has been changed to default port.`	An administrator changed the port number for SSH back to the default (22).
`SSH certificate:%s does not exist. SSH service will not work.`	An administrator assigned a nonexistent certificate to SSH. %s is certificate name assigned by user
`SSH certificate:%s format is wrong. SSH service will not work.`	After an administrator assigns a certificate for SSH, the device needs to convert it to a key used for SSH. %s is certificate name assigned by user
`TELNET port has been changed to port %s.`	An administrator changed the port number for TELNET. %s is port number assigned by user
`TELNET port has been changed to default port.`	An administrator changed the port number for TELNET back to the default (23).
`FTP certificate:%s does not exist.`	An administrator assigned a nonexistent certificate to FTP. %s is certificate name assigned by user
`FTP port has been changed to port %s.`	An administrator changed the port number for FTP. %s is port number assigned by user
`FTP port has been changed to default port.`	An administrator changed the port number for FTP back to the default (21).
`SNMP port has been changed to port %s.`	An administrator changed the port number for SNMP. %s is port number assigned by user
`SNMP port has been changed to default port.`	An administrator changed the port number for SNMP back to the default (161).

Table 247 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`Console baud has been changed to %s.`	An administrator changed the console port baud rate. %s is baud rate assigned by user
`Console baud has been reset to %d.`	An administrator changed the console port baud rate back to the default (115200). %d is default baud rate
`DHCP Server on Interface %s will not work due to Device HA status is Stand-By`	If interface is stand-by mode for device HA, DHCP server can't be run. Otherwise it has conflict with the interface in master mode. %s is interface name
`DHCP Server on Interface %s will be reapplied due to Device HA status is Active`	When an interface has become the HA master, the DHCP server needs to start operating. %s is interface name
`DHCP's DNS option:%s has changed.`	DHCP pool's DNS option support from WAN interface. If this interface is unlink/disconnect or link/connect, this log will be shown. %s is interface name. The DNS option of DHCP pool has retrieved from it
`Set timezone to %s.`	An administrator changed the time zone. %s is time zone value
`Set timezone to default.`	An administrator changed the time zone back to the default (0).
`Enable daylight saving.`	An administrator turned on daylight saving.
`Disable daylight saving.`	An administrator turned off daylight saving.
`DNS access control rules have been reached the maximum number.`	An administrator tried to add more than the maximum number of DNS access control rules (64).
`DNS access control rule %u of DNS has been appended.`	An administrator added a new rule. %u is rule number
`DNS access control rule %u has been inserted.`	An administrator inserted a new rule. %u is rule number
`DNS access control rule %u has been appended`	An administrator appended a new rule. %u is rule number
`DNS access control rule %u has been modified`	An administrator modified the rule %u. %u is rule number
`DNS access control rule %u has been deleted.`	An administrator removed the rule %u. %u is rule number
`DNS access control rule %u has been moved to %d.`	An administrator moved the rule %u to index %d. %u is previous index %d variable is current index

Table 247 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`The default record of Zone Forwarder have reached the maximum number of 128 DNS servers.`	The default record DNS servers is more than 128.
`Interface %s ping check is successful. Zone Forwarder adds DNS servers in records.`	Ping check ok, add DNS servers in bind. %s is interface name
`Interface %s ping check is failed. Zone Forwarder removes DNS servers in records.`	Ping check failed, remove DNS servers from bind. %s is interface name
`Interface %s ping check is disabled. Zone Forwarder adds DNS servers in records.`	Ping check disabled, add DNS servers in bind. %s is interface name
`Wizard apply DNS server failed.`	Wizard apply DNS server failed.
`Wizard adds DNS server %s failed because DNS zone setting has conflictd.`	Wizard apply DNS server failed because DNS zone conflicted. %s is the IP address of the DNS server
`Wizard adds DNS server %s failed because Zone Forwarder numbers have reached the maximum number of 32.`	Wizard apply DNS server fail because the device already has the maximum number of DNS records configured. %s is IP address of the DNS server.
`Access control rules of %s have reached the maximum number of %u`	The maximum number of allowable rules has been reached. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. %u is the maximum number of access control rules.
`Access control rule %u of %s was appended.`	A new built-in service access control rule was appended. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was inserted.`	An access control rule was inserted successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was modified.`	An access control rule was modified successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was deleted.`	An access control rule was removed successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.

Table 247 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`Access control rule %d of %s was moved to %d.`	An access control rule was moved successfully. 1st %d is the previous index . %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. 2nd %d is current previous index.
`SNMP trap can not be sent successfully`	Cannot send a SNMP trap to a remote host due to network error

Table 248 System Logs

LOG MESSAGE	DESCRIPTION
`Port %d is up!!`	When LINK is up, %d is the port number.
`Port %d is down!!`	When LINK is down, %d is the port number.
`%s is dead at %s`	A daemon (process) is gone (was killed by the operating system). 1st %s: Daemon Name, 2nd %s: date+time
`%s process count is incorrect at %s`	The count of the listed process is incorrect. 1st %s: Daemon Name, 2nd %s: date+time
`%s becomes Zombie at %s`	A process is present but not functioning. 1st %s: Daemon Name, 2nd %s: date+time When memory usage exceed threshold-max, memory usage reaches %d%% :mem-threshold-max. When disk usage exceeds threshold-max, %s: Partition name file system usage reaches %d%%: disk-threshold-max. When memory usage drops below threshold-min, System Memory usage drops below the threshold of %d%%: mem-threshold-min. When disk usage drops below threshold-min, %s: partition_name file system drops below the threshold of %d%%: disk-threshold-min.
`DHCP Server executed with cautious mode enabled`	DHCP Server executed with cautious mode enabled.
`DHCP Server executed with cautious mode disabled`	DHCP Server executed with cautious mode disabled.
`Received packet is not an ARP response packet`	A packet was received but it is not an ARP response packet.
`Receive an ARP response`	The device received an ARP response.
`Receive ARP response from %s (%s)`	The device received an ARP response from the listed source.
`The request IP is: %s, sent from %s`	The device accepted a request.
`Received ARP response NOT for the request IP address`	The device received an ARP response that is NOT for the requested IP address.
`Receive an ARP response from the client issuing the DHCP request`	The device received an ARP response from the client issuing the DHCP request.

Table 248 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`Receive an ARP response from an unknown client`	The device received an ARP response from an unknown client.
`In total, received %d arp response packets for the requested IP address`	The device received the specified total number of ARP response packets for the requested IP address.
`Clear arp cache successfully.`	The ARP cache was cleared successfully.
`Client MAC address is not an Ehernet address`	A client MAC address is not an Ethernet address.
`DHCP request received via interface %s (%s:%s), src_mac: %s with requested IP: %s`	The device received a DHCP request through the specified interface.
`IP confliction is detected. Send back DHCP-NAK.`	IP conflict was detected. Send back DHCP-NAK.
`Clear ARP cache done`	Clear ARP cache done.
`NTP update successful, current time is %s`	The device successfully synchronized with a NTP time server . %s is the time format.
`NTP update failed`	The device was not able to synchronize with the NTP time server successfully.
`Device is rebooted by administrator!`	An administrator restarted the device.
`Insufficient memory.`	Cannot allocate system memory.
`Connect to dyndns server has failed.`	Cannot connect to members.dyndns.org to update DDNS.
`Update the profile %s has failed because of strange server response.`	Update profile failed because the response was strange, %s is the profile name.
`Update the profile %s has succeeded because the IP address of FQDN %s was not changed.`	Update profile succeeded, because the IP address of profile is unchanged, %s is the profile name.
`Update the profile %s has succeeded.`	Update profile succeeded, %s is the profile name.
`Update the profile %s has failed because the FQDN %s is invalid.`	Update profile failed because FQDN for the profile is invalid for DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s is malformed.`	The FQDN format is malformed for DynDNS server, 1st %s is the profile name, 2nd %s is the FQDN of the profile.

Table 248 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`Update the profile %s has failed because the FQDN %s is not under your control.`	The owner of this FQDN is not the user, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s was blocked for abuse.`	The FQDN is blocked by DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because of authentication fail.`	Try to update profile, but failed, because of authentication fail, %s is the profile name.
`Update the profile %s has failed because of invalid system parameters.`	Some system parameters are invalid to update FQDN, %s is the profile name.
`Update the profile %s has failed because the FQDN %s was blocked.`	The FQDN is blocked by DynDNS , 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because too many or too few hosts found.`	%s is the profile name.
`Update the profile %s has failed because of dyndns internal error`	Update profile failed because of a dynsdns internal error, %s is the profile name.
`Update the profile %s has failed because the feature requested is only available to donators.`	Update profile failed because the feature requested is only available to donators, %s is the profile name.
`Update the profile %s has failed because of error response.`	Update profile failed because the response is incorrect, %s is the profile name.
`Update the profile %s has failed because %s.`	Update profile failed, and show the response message, 1st %s is the profile name, 2nd %s is the reason.
`Update the profile %s has failed because of unknown error.`	Update profile failed because unknown error. Sometimes, the force authentication will result in this error, 1st %s is the profile name.
`Update the profile %s has failed because Username was empty.`	DDNS profile needs username, %s is the profile name.
`Update the profile %s has failed because Password was empty.`	DDNS profile needs password, %s is the profile name.
`Update the profile %s has failed because Domain name was empty.`	DDNS profile needs domain name, %s is the profile name.

Table 248 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`Update the profile %s has failed because Custom IP was empty.`	The DDNS profile's IP select type is custom, and a custom IP was not defined, %s is the profile name.
`Update the profile %s has failed because WAN interface was empty.`	If the DDNS profile's IP select type is iface, it needs a WAN iface, %s is the profile name.
`The profile %s has been paused because the VRRP status of WAN interface was standby.`	The profile is paused by device-HA, because the VRRP status of that iface is standby, %s is the profile name.
`Update the profile %s has failed because WAN interface was link-down.`	DDNS profile cannot be updated for WAN IP because WAN iface is link-down, %s is the profile name.
`Update the profile %s has failed because WAN interface was not connected.`	DDNS profile cannot be updated for WAN IP because WAN iface is PPP and not connected, %s is the profile name.
`Update the profile %s has failed because IP address of WAN interface was empty.`	DDNS profile cannot be updated because the IP of WAN iface is 0.0.0.0, 1st %s is the profile name.
`Update the profile %s has failed because ping-check of WAN interface has failed.`	DDNS profile cannot be updated because the ping-check for WAN iface failed , %s is the profile name.
`The profile %s has been paused because the HA interface of VRRP status was standby.`	The profile is paused by Device-HA, because the VRRP status of that HA iface is standby, %s is the profile name.
`Update the profile %s has failed because HA interface was link-down.`	DDNS profile cannot be updated for HA IP address because HA iface is link-down, %s is the profile name.
`Update the profile %s has failed because the HA interface was not connected.`	DDNS profile cannot be updated for HA IP address because HA iface is PPP and not connected, %s is the profile name.
`Update the profile %s has failed because IP address of HA interface was empty.`	DDNS profile cannot be updated because the IP address of HA iface is 0.0.0.0, %s is the profile name.
`Update the profile %s has failed because ping-check of HA interface has failed.`	DDNS profile cannot be updated because the fail of ping-check for HA iface, %s is the profile name
`DDNS has been disabled by Device-HA.`	DDNS is disabled by Device-HA, because all VRRP groups are standby.

Table 248 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`DDNS has been enabled by Device-HA.`	DDNS is enabled by Device-HA, because one of VRRP groups is active.
`Disable DDNS has succeeded.`	Disable DDNS.
`Enable DDNS has succeeded.`	Enable DDNS.
`DDNS profile %s has been renamed as %s.`	Rename DDNS profile, 1st %s is the original profile name, 2nd %s is the new profile name.
`DDNS profile %s has been deleted.`	Delete DDNS profile, %s is the profile name,
`DDNS Initialization has failed.`	Initialize DDNS failed,
`All DDNS profiles are deleted`	All DDNS profiles have been removed.

Table 249 Connectivity Check Logs

LOG MESSAGE	DESCRIPTION
`Cann't open link_up2`	Can not recover routing status which is link-down.
`Can not open %s.pid`	Can not open connectivity check process ID file. %s: interface name
`Can not open %s.arg`	Can not open configuration file for connectivity check process. %s: interface name
`The connectivity-check is activate for %s interface`	The link status of interface is still activate after check of connectivity check process. %s: interface name
`The connectivity-check is fail for %s interface`	The link status of interface is fail after check of connectivity check process. %s: interface name
`Can't get gateway IP of %s interface`	The connectivity check process can't get the gateway IP address for the specified interface. %s: interface name
`Can't alloc memory`	The connectivity check process can't get memory from OS.
`Can't load %s module`	The connectivity check process can't load module for check link-status. %s: the connectivity module, currently only ICMP available.
`Can't handle 'isalive' function of %s module`	The connectivity check process can't execute 'isalive' function from module for check link-status. %s: the connectivity module, currently only ICMP available.
`Create socket error`	The connectivity check process can't get socket to send packet.
`Can't get IP address of %s interface`	The connectivity check process can't get IP address of interface. %s: interface name.
`Can't get flags of %s interface`	The connectivity check process can't get interface configuration. %s: interface name

Table 249 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
`Can't get remote address of %s interface`	The connectivity check process can't get remote address of PPP interface %s: interface name
`Can't get NETMASK address of %s interface`	The connectivity check process can't get netmask address of interface. %s: interface name
`Can't get BROADCAST address of %s interface`	The connectivity check process can't get broadcast address of interface %s: interface name
`Can't use MULTICAST IP for destination`	The connectivity check process can't use multicast address to check link-status.
`The destination is invalid, because destination IP is broadcast IP`	The connectivity check process can't use broadcast address to check link-status.
`Can't get MAC address of %s interface!`	The connectivity check process can't get MAC address of interface. %s: interface name
`To send ARP REQUEST error!`	The connectivity check process can't send ARP request packet.
`The %s routing status seted to DEAD by connectivity-check`	The interface routing can't forward packet. %s: interface name
`The %s routing status seted ACTIVATE by connectivity-check`	The interface routing can forward packet. %s: interface name

Table 250 Device HA Logs

LOG MESSAGE	DESCRIPTION
`Device HA VRRP Group %s has been added.`	An VRRP group has been created, %s: the name of VRRP group.
`Device HA VRRP group %s has been modified.`	An VRRP group has been modified, %s: the name of VRRP group.
`Device HA VRRP group %s has been deleted.`	An VRRP group has been deleted, %s: the name of VRRP group.
`Device HA VRRP interface %s for VRRP Group %s has changed.`	Configuration of an interface that belonged to a VRRP group has been changed, 1st %s: VRRP interface name, 2ed %s: %s: the name of VRRP group.
`Device HA syncing from %s starts.`	Device HA Syncing from Master starts when user click "Sync Now" using Auto Sync, %s: The IP of FQDN of Master.
`%s has no file to sync, Skip syncing it for %s.`	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2ed %s: The feature name for the syncing object.

Table 250 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
`Master configuration is the same with Backup. Skip updating it.`	The System Startup configuration file synchronized from the Master is the same with the one in the Backup, so the configuration does not have to be updated.
`%s file not existed, Skip syncing it for %s`	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2ed %s: The feature name for the syncing object.
`Master firmware version can not be recognized. Stop syncing from Master.`	Synchronizing stopped because the firmware version file was not found in the Master. A Backup device only synchronizes from the Master if the firmware versions are the same between the Master and the Backup.
`Device HA Sync has failed when syncing %s for %s due to bad \"Sync Password\".`	The synchronization password was incorrect when attempting to synchronize a certain object (AV/AS/IDP/Certificate/System Configuration). 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
`Device HA Sync has failed when syncing %s for %s due to bad \"Sync From\" or \"Sync Port\".`	The Sync From IP address or Sync Port may be incorrect when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration).
`Device HA Sync has failed when syncing %s for %s.`	Synchronization failed when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration) due to an unknown reason, 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
`Sync Failed: Cannot connect to Master when syncing %s for %s.`	Synchronization failed because the Backup could not connect to the Master. The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
`Backup firmware version can not be recognized. Stop syncing from Master.`	The firmware version on the Backup cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
`Sync failed: Remote Firmware Version Unknown`	The firmware version on the Master cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
`Master firmware version should be the same with Backup.`	The Backup and Master have different firmware versions. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
`Update %s for %s has failed.`	Updating a certain object failed when updating (AS/AV/IDP/Certificate/System Configuration). 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
`Update %s for %s has failed: %s.`	Updating a certain object failed when updating (AS/AV/IDP/Certificate/System Configuration) due to some reason. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
`Device HA has skipped syncing %s since %s is %s.`	A certain service has no license or the license is expired, so it was not synchronized from the Master. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized, 3rd %s: unlicensed or license expired.

Table 250 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
`Device HA authentication type for VRRP group %s maybe wrong.`	A VRRP group's Authentication Type (Md5 or IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
`Device HA authenticaton string of text for VRRP group %s maybe wrong.`	A VRRP group's Simple String (Md5) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
`Device HA authentication string of AH for VRRP group %s maybe wrong.`	A VRRP group's AH String (IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
`Retrying to update %s for %s. Retry: %d.`	An update failed. Retrying to update the failed object again. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized, %d: the retry count.
`Recovring to Backup original state for %s has failed.`	An update failed. The device will try to recover the failed update feature to the original state before Device HA synchronizes the specified object.
`Recovering to Backup original state for %s has succeeded.`	Recovery succeeded when an update for the specified object failed.
`One of VRRP groups has became avtive. Device HA Sync has aborted from Master %s.`	%s: IP or FQDN of Master
`Master configuration file does not exist. Skip updating ZySH Startup Configuration.`	
`System internal error: %s. Skip updating %s.`	1st %s: error string, 2ed %s: the syncing object
`Master configuration file is empty. Skip updating ZySH Startup Configuration.`	
`Device HA Sync has failed when syncing %s for %s due to transnission timeout.`	1st %s: the syncing object, 2ed %s: the feature name for the syncing object

Table 251 Routing Protocol Logs

LOG MESSAGE	DESCRIPTION
`RIP on interface %s has been stopped because Device-HA binds this interface.`	Device-HA is currently running on the interface %s, so all the local service have to be stopped including RIP. %s: Interface Name
`RIP on all interfaces have been stopped`	Got the CLI command 'no router rip' to shut down RIP on all interfaces
`Invalid RIP md5 authentication`	RIP md5 authentication has been set without setting md5 authentication id and key first
`Invalid RIP text authentication.`	RIP text authentication has been set without setting authentication key first
`RIP on interface %s has been activated.`	RIP on interface %s has been activated. %s: Interface Name
`RIP direction on interface %s has been changed to In-Only.`	RIP direction on interface %s has been changed to In-Only. %s: Interface Name
`RIP direction on interface %s has been changed to Out-Only.`	RIP direction on interface %s has been changed to Out-Only. %s: Interface Name
`RIP authentication mode has been changed to %s.`	RIP authentication mode has been changed to text or md5.
`RIP text authentication key has been changed.`	RIP text authentication key has been changed.
`RIP md5 authentication id and key have been changed.`	RIP md5 authentication id and key have been changed.
`RIP global version has been changed to %s.`	RIP global version has been changed to version 1 or 2.
`RIP redistribute OSPF routes has been enabled.`	RIP redistribute OSPF routes has been enabled.
`RIP redistribute static routes has been enabled.`	RIP redistribute static routes has been enabled.
`RIP on interface %s has been deactivated.`	RIP on interface %s has been deactivated. %s: Interface Name
`RIP direction on interface %s has been changed to BiDir.`	RIP direction on interface %s has been changed to BiDir. %s: Interface Name
`RIP authentication has benn disabled.`	RIP text or md5 authentication has been disabled.
`RIP text authentication key has been deleted.`	RIP text authentication key has been deleted.

Table 251 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
`RIP md5 authentication id and key have been deleted.`	RIP md5 authentication id and key have been deleted.
`RIP global version has been deleted.`	RIP global version has been deleted.
`RIP redistribute OSPF routes has been disabled.`	RIP redistribute OSPF routes has been disabled.
`RIP redistribute static routes has been disabled.`	RIP redistribute static routes has been disabled.
`RIP v2-broadcast on interface %s has been enabled.`	RIP v2-broadcast on interface %s has been enabled. %s: Interface Name.
`RIP send-version on interface %s has been changed to %s.`	RIP send-version on interface %s has been changed to version 1 or 2 or both 1 2. %s: Interface Name.
`RIP receive-version on interface %s has been changed to %s.`	RIP receive-version on interface %s has been changed to version 1 or 2 or both 1 2. 2nd%s: Interface Name.
`RIP send-version on interface %s has been reset to current global version %s.`	RIP send-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP Version
`RIP receive-version on interface %s has been reset to current global version %s.`	RIP receive-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP
`RIP v2-broadcast on interface %s has been disabled.`	RIP v2-broadcast on interface %s has been disabled. %s: Interface Name
`OSPF on interface %s has been stopped because Device-HA binds this interface.`	Device-HA is currently running on the interface %s, so all the local service have to be stopped including OSPF. %s: Interface Name
`Area %s cannot be removed. This area is in use.`	One or more interfaces are still using this area, so area %s cannot be removed. %s: OSPF Area
`Invalid OSPF %s authentication of area %s.`	OSPF md5 or text authentication has been set without setting md5 authentication id and key, or text authentication key first.
`Invalid OSPF virtual-link %d md5 authentication of area %s.`	Virtual-link %s md5 authentication has been set without setting md5 authentication id and key first. %s: Virtual-Link ID
`Invalid OSPF virtual-link %s text authentication of area %s.`	Virtual-link %s text authentication has been set without setting text authentication key first. %s: Virtual-Link ID

Table 251 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
`Invalid OSPF virtual-link %s authentication of area %s.`	Virtual-link %s authentication has been set to same-as-area but the area has invalid authentication configuration. %s: Virtual-Link ID
`Invalid OSPF md5 authentication on interface %s.`	Invalid OSPF md5 authentication is set on interface %s. %s: Interface Name
`Invalid OSPF text authentication on interface %s.`	Invalid OSPF text authentication is set on interface %s. %s: Interface Name
`Interface %s does not belong to any OSPF area.`	Interface %s has been set OSPF authentication same-as-area, however the interface does not belong to any OSPF area. %s: Interface Name
`Invalid OSPF authentication of area %s on interface %s.`	Interface %s has been set OSPF authentication same-as-area, however the area has invalid text authentication configuration. %s: Interface Name

Table 252 NAT Logs

LOG MESSAGE	DESCRIPTION
`The NAT range is full`	The NAT mapping table is full.
`%s FTP ALG has succeeded.`	The FTP Application Layer Gateway (ALG) has been turned on or off. %s: Enable or Disable
`Extra signal port of FTP ALG has been modified.`	Extra FTP ALG port has been changed.
`Signal port of FTP ALG has been modified.`	Default FTP ALG port has been changed.
`%s H.323 ALG has succeeded.`	The H.323 ALG has been turned on or off. %s: Enable or Disable
`Extra signal port of H.323 ALG has been modified.`	Extra H.323 ALG port has been changed.
`Signal port of H.323 ALG has been modified.`	Default H.323 ALG port has been changed.
`%s SIP ALG has succeeded.`	The SIP ALG has been turned on or off. %s: Enable or Disable
`Extra signal port of SIP ALG has been modified.`	Extra SIP ALG port has been changed.
`Signal port of SIP ALG has been modified.`	Default SIP ALG port has been changed.
`Register SIP ALG extra port=%d failed.`	SIP ALG apply additional signal port failed. %d: Port number
`Register SIP ALG signal port=%d failed.`	SIP ALG apply signal port failed. %d: Port number

Table 252 NAT Logs (continued)

LOG MESSAGE	DESCRIPTION
`Register H.323 ALG extra port=%d failed.`	H323 ALG apply additional signal port failed. %d: Port number
`Register H.323 ALG signal port=%d failed.`	H323 ALG apply signal port failed. %d: Port number
`Register FTP ALG extra port=%d failed.`	FTP ALG apply additional signal port failed. %d: Port number
`Register FTP ALG signal port=%d failed.`	FTP ALG apply signal port failed. %d: Port number

Table 253 PKI Logs

LOG MESSAGE	DESCRIPTION
`Generate X509certifiate "%s" successfully`	The router created an X509 format certificate with the specified name.
`Generate X509 certifiate "%s" failed, errno %d`	The router was not able to create an X509 format certificate with the specified name. See Table 254 on page 698 for details about the error number.
`Generate certifiate request "%s" successfully`	The router created a certificate request with the specified name.
`Generate certifiate request "%s" failed, errno %d`	The router was not able to create a certificate request with the specified name. See Table 254 on page 698 for details about the error number.
`Generate PKCS#12 certificate "%s" successfully`	The router created a PKCS#12 format certificate with the specified name.
`Generate PKCS#12 certificate "%s" failed, errno %d`	The router was not able to create anPKCS#12 format certificate with the specified name. See Table 254 on page 698 for details about the error number.
`Prepare to import "%s" into "My Certificate"`	%s is the name of a certificate request.
`Prepare to import "%s" into Trusted Certificate"`	%s is the name of a certificate request.
`CMP enrollment "%s" successfully, CA "%s", URL "%s"`	The device used CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
`CMP enrollment "%s" failed, CA "%s", URL "%s"`	The device was unable to use CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
`SCEP enrollment "%s" successfully, CA "%s", URL "%s"`	The device used SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
`SCEP enrollment "%s" failed, CA "%s", URL "%s"`	The device was unable to use SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL

Table 253 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Import X509 certificate "%s" into My Certificate successfully`	The device imported a x509 format certificate into My Certificates. %s is the certificate request name.
`Import X509 certificate "%s" into Trusted Certificate successfully`	The device imported a x509 format certificate into Trusted Certificates. %s is the certificate request name.
`Import PKCS#12 certificate "%s" into "My Certificate" successfully`	The device imported a PKCS#12 format certificate into My Certificates. %s is the certificate request name.
`Import PKCS#7 certificate "%s" into "My Certificate" successfully`	The device imported a PKCS#7 format certificate into My Certificates. %s is the certificate request name.
`Import PKCS#7 certificate "%s" into "Trusted Certificate" successfully`	The device imported a PKCS#7 format certificate into Trusted Certificates. %s is the certificate request name.
`Decode imported certificate "%s" failed`	The device was not able to decode an imported certificate. %s is certificate the request name
`Export PKCS#12 certificate "%s" from "My Certificate" successfully`	The device exported a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
`Export PKCS#12 certificate "%s" from "My Certificate" failed`	The device was not able to export a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "My Certificate" failed`	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "Trusted Certificate" failed`	The device was not able to export a x509 format certificate from Trusted Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "My Certificate" successfully`	The device exported a x509 format certificate from My Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "Trusted Certificate" successfully`	The device exported a x509 format certificate from Trusted Certificates. %s is the certificate request name.

Table 253 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Export X509 certificate "%s" from "My Certificate" failed`	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
`Import PKCS#12 certificate "%s" with incorrect password`	An administrator used the wrong password when trying to import a PKCS#12 format certificate. %s is the certificate name.
`Cert trusted: %s`	%s is the subject.
`Due to %d, cert not trusted: %s`	%d is an error number (see Table 254 on page 698), %s is the certificate subject.

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.

CODE	DESCRIPTION
`27`	Path was not verified.
`28`	Maximum path length reached.

Table 254 Interface Logs

LOG MESSAGE	DESCRIPTION
`Interface %s has been deleted.`	An administrator deleted an interface. %s is the interface name.
`AUX Interface dialing failed. This AUX interface is not enabled.`	A user tried to dial the AUX interface, but the AUX interface is not enabled.
`AUX Interface disconnecting failed. This AUX interface is not enabled.`	The AUX interface is not enabled and a user tried to use the disconnect aux command.
`Please type phone number of interface AUX first then dial again.`	A user tried to dial the AUX interface, but the AUX interface does not have a phone number set.
`Please type phone number of Interface AUX first then disconnect again.`	The AUX interface does not have a phone number set and a user tried to use the disconnect aux command.
`Interface %s will reapply because Device HA become active status.`	Device-ha became active and is using a PPP base interface, the PPP interface must reapply, %s is the interface name.
`Interface %s will reapply because Device HA is not running.`	Device-ha was deleted and free PPP base interface, PPP interface must reapply, %s is the interface name.
`Interface %s will stop connect because Device HA become standby status.`	When device-ha is stand-by and use PPP base interface, PPP interface connection will stop, `%s`: interface name.
`Create interface %s has been failed.`	When PPP can't running fail, `%s`: interface name.
`Base interface %s is disabled. Interface %s is disabled now.`	When user disable ethernet, vlan or bridge interface and this interface is base interface of PPP or virtual interface. PPP and virtual will disable too. 1st %s is interface name, 2nd %s is interface.
`Interface %s has been changed.`	An administrator changed an interface's configuration. `%s`: interface name.
`Interface %s has been added.`	An administrator added a new interface. `%s`: interface name.
`Interface %s is enabled.`	An administrator enabled an interface. %s: interface name.
`Interface %s is disabled.`	An administrator disabled an interface. %s: interface name.

Table 254 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`%s MTU > (%s MTU - 8), %s may not work correctly.`	An administrator configured a PPP interface, PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface ans peer will not receive correct PPP packets. 1st %s: PPP interface name, 2nd %s: ethernet interface name.
`(%s MTU - 8) < %s MTU, %s may not work correctly.`	An administrator configured ethernet, vlan or bridge and this interface is base interface of PPP interface. PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and peer will not receive correct PPP packets.1st %s: Ethernet interface name, 2nd %s: PPP interface name.
`Interface %s links down. Default route will not apply until interface %s links up.`	An administrator set a static gateway in interface but this interface is link down. At this time the configuration will be saved but route will not take effect until the link becomes up.1st %s: interface name, 2nd %s: interface name.
`name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u,UpTime=%s`	Port statistics log. This log will be sent to the VRPT server. 1st %s: physical port name, 2nd %s: physical port status, 1st %u: physical port Tx packets, 2nd %u: physical port Rx packets, 3rd %u: physical port packets collisions, 4th %u: physical port Tx Bytes/s, 5th %u: physical port Rx Bytes/s, 3rd %s: physical port up time.
`name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u`	Interface statistics log. This log will be sent to the VRPT server. 1st %s: interface name, 2nd %s: interface status, 1st %u variable: interface Tx packets, 2nd %u variable: interface Rx packets, 3rd %u: interface packets collisions, 4th %u: interface Tx Bytes/s, 5th %u: interface Rx Bytes/s.
`Interface %s start dailing.`	A PPP or aux interface started dialing to a server. %s: interface name.
`Interface %s connect failed: Connect to server failed.`	A PPTP interface failed to connect to the PPTP server. %s: interface name.
`Interface %s connection terminated.`	A PPP or AUX connection will terminate. %s: interface name.
`Interface %s connection terminated: idle timeout.`	An idle PPP or AUX connection timed out.1%s: interface name.
`Interface %s connect failed: MS-CHAPv2 mutual authentication failed.`	MS-CHAPv2 authentication failed (the server must support mS-CHAPv2 and verify that the authentication failed, this does not include cases where the servers does not support MS-CHAPv2). %s: interface name.
`Interface %s connect failed: MS-CHAP authentication failed.`	MS-CHAP authentication failed (the server must support MS-CHAP and verify that the authentication failed, this does not include cases where the server does not support MS-CHAP). %s: interface name.
`Interface %s connect failed: CHAP authentication failed.`	CHAP authentication failed (the server must support CHAP and verify that the authentication failed, this does not include cases where the server does not support CHAP). CHAP: interface name.
`Interface %s is connected.`	A PPP or AUX interface connected successfully. %s: interface name.

Table 254 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`Interface %s is disconnected.`	A PPP or AUX interface disconnected successfully. %s: interface name.
`Interface %s connect failed: Peer not responding.`	The interface's connection will be terminated because the server did not send any LCP packets. %s: interface name.
`Interface %s connect failed: PAP authentication failed.`	PAP authentication failed (the server must support PAP and verify verify that the authentication failed, this does not include cases where the server does not support PAP). %s: PPP interface name.
`Interface %s connect failed: Connect timeout.`	A PPPOE connection timed out due to a lack of response from the PPPOE server. %s: PPP interface name.
`Interface %s create failed because has no member.`	A bridge interface has no member. %s: bridge interface name.

Table 255 Account Logs

LOG MESSAGE	DESCRIPTION
`Account %s %s has been deleted.`	A user deleted an ISP account profile. 1st %s: profile type, 2nd %se: profile name.
Account %s %s has been changed.	A user changed an ISP account profile's options. 1st %s: profile type, 2nd %s: profile name.
Account %s %s has been added.	A user added a new ISP account profile. 1st %s: profile type, 2nd %s: profile name.

Table 256 Port Grouping Logs

LOG MESSAGE	DESCRIPTION
`Interface %s links up because of changing Port Group. Enable DHCP client.`	An administrator used port-grouping to assign a port to a representative Interface and this representative interface is set to DHCP client and only has one member. In this case the DHCP client will be enabled. %s: interface name.
`Interface %s links down because of changing Port Group. Disable DHCP client.`	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has no members in its group. In this case the DHCP client will be disabled. %s: interface name.
`Port Group on %s is changed. Renew DHCP client.`	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has more than one member in its group. In this case the DHCP client will renew. %s: interface name.
`Port Grouping %s has been changed.`	An administrator configured port-grouping, %s: interface name.

Table 257 Force Authentication Logs

LOG MESSAGE	DESCRIPTION
`Force User Authentication will be enabled due to http server is enabled.`	Force user authentication will be turned on because HTTP server was turned on.
`Force User Authentication will be disabled due to http server is disabled.`	Force user authentication will be turned off because HTTP server was turned off.
`Force User Authentication may not work properly!`	

Table 258 File Manager Logs

LOG MESSAGE	DESCRIPTION
`ERROR:#%s, %s`	Apply configuration failed, this log will be what CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
`WARNING:#%s, %s`	Apply configuration failed, this log will be what CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
`ERROR:#%s, %s`	Run script failed, this log will be what wrong CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
`WARNING:#%s, %s`	Run script failed, this log will be what wrong CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
`Resetting system...`	Before apply configuration file.
`System resetted. Now apply %s..`	After the system reset, it started to apply the configuration file. %s is configuration file name.
`Running %s...`	An administrator ran the listed shell script. %s is script file name.

C

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 259 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 259 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.

Table 259 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

D

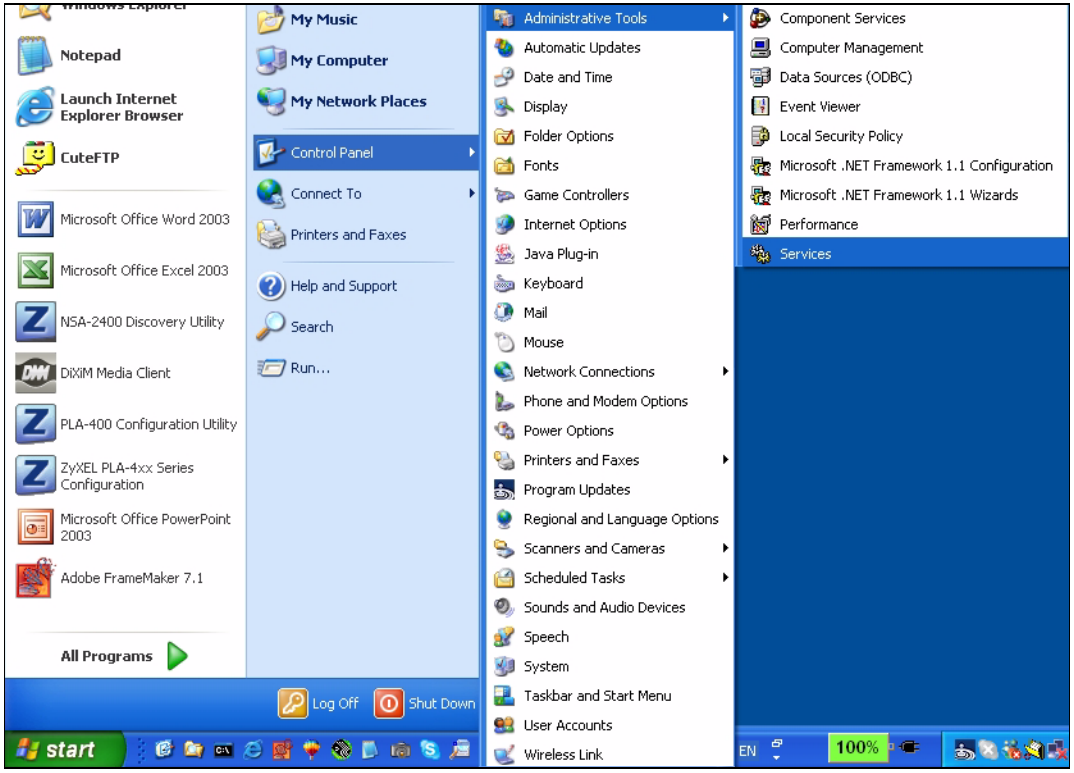
Displaying Anti-Virus Alert Messages in Windows

With the anti-virus packet scan, when a virus is detected, you can have the ZyWALL display an alert message on Miscrosoft Windows-based computers. If the log shows that virus files are being detected but your Miscrosoft Windows-based computer is not displaying an alert message, use one of the following procedures to make sure your computer is set to display the messages.

Windows XP

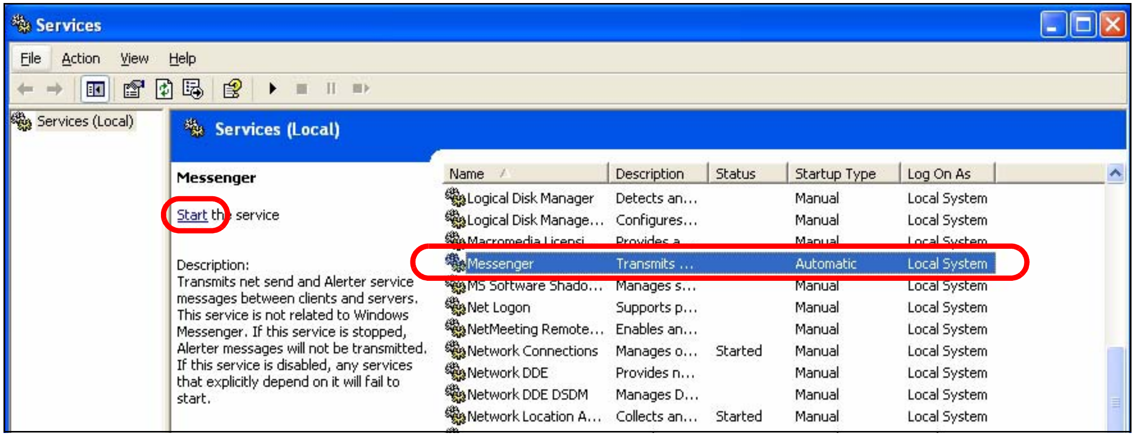
1 Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Figure 483 Windows XP: Opening the Services Window


Windows Explorer
Notepad
Launch Internet Explorer Browser
CuteFTP
Microsoft Office Word 2003
Microsoft Office Excel 2003
NSA-2400 Discovery Utility
DiXiM Media Client
PLA-400 Configuration Utility
ZyXEL PLA-4xx Series Configuration
Microsoft Office PowerPoint 2003
Adobe FrameMaker 7.1
All Programs
My Music
My Computer
My Network Places
Control Panel
Connect To
Printers and Faxes
Help and Support
Search
Run...
Log Off
Shut Down
start
Administrative Tools
Automatic Updates
Date and Time
Display
Folder Options
Fonts
Game Controllers
Internet Options
Java Plug-in
Keyboard
Mail
Mouse
Network Connections
Phone and Modem Options
Power Options
Printers and Faxes
Program Updates
Regional and Language Options
Scanners and Cameras
Scheduled Tasks
Sounds and Audio Devices
Speech
System
Taskbar and Start Menu
User Accounts
Wireless Link
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
Local Security Policy
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Performance
Services
EN
100%

2 Select the **Messenger** service and click **Start**.

Figure 484 Windows XP: Starting the Messenger Service


Services
File
Action
View
Help
Services (Local)
Services (Local)
Messenger
Start the service

Description:
Transmits net send and Alerter service messages between clients and servers. This service is not related to Windows Messenger. If this service is stopped, Alerter messages will not be transmitted. If this service is disabled, any services that explicitly depend on it will fail to start.

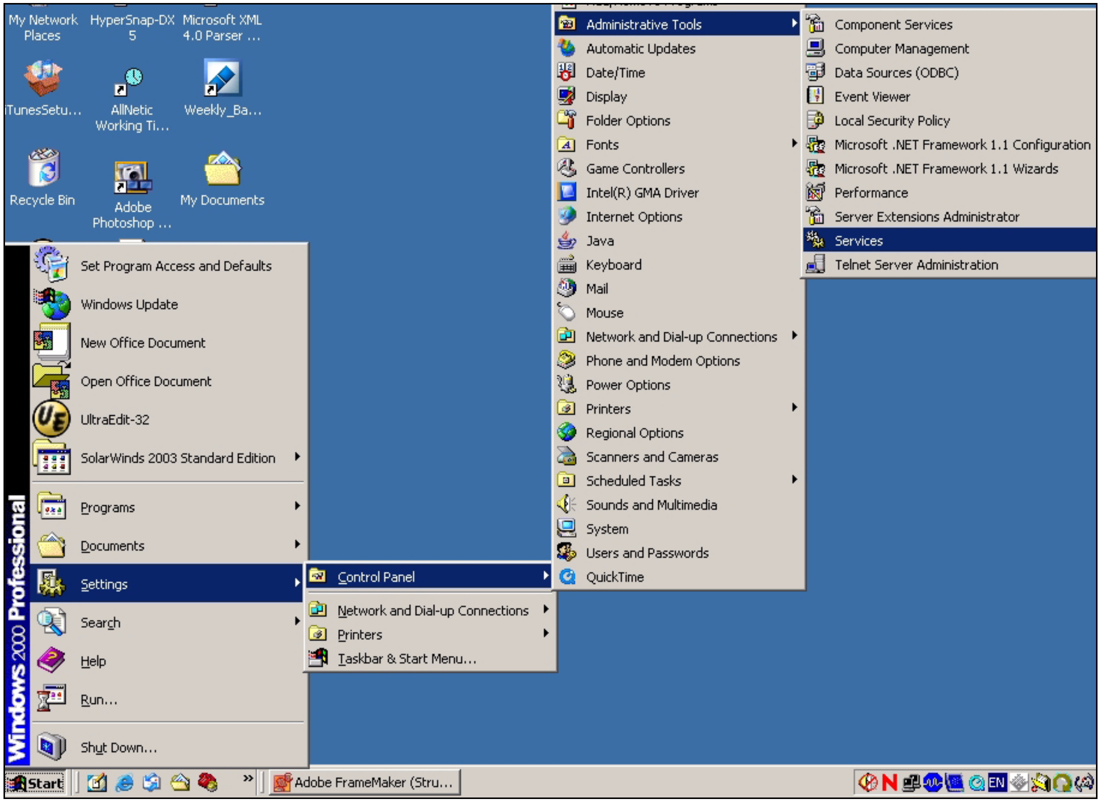
Name	Description	Status	Startup Type	Log On As
Logical Disk Manager	Detects an...		Manual	Local System
Logical Disk Manage...	Configures...		Manual	Local System
Macromedia Licensi...	Provides a...		Manual	Local System
Messenger	Transmits ...		Automatic	Local System
MS Software Shado...	Manages s...		Manual	Local System
Net Logon	Supports p...		Manual	Local System
NetMeeting Remote...	Enables an...		Manual	Local System
Network Connections	Manages o...	Started	Manual	Local System
Network DDE	Provides n...		Manual	Local System
Network DDE DSDM	Manages D...		Manual	Local System
Network Location A...	Collects an...	Started	Manual	Local System

3 Close the window when you are done.

Windows 2000

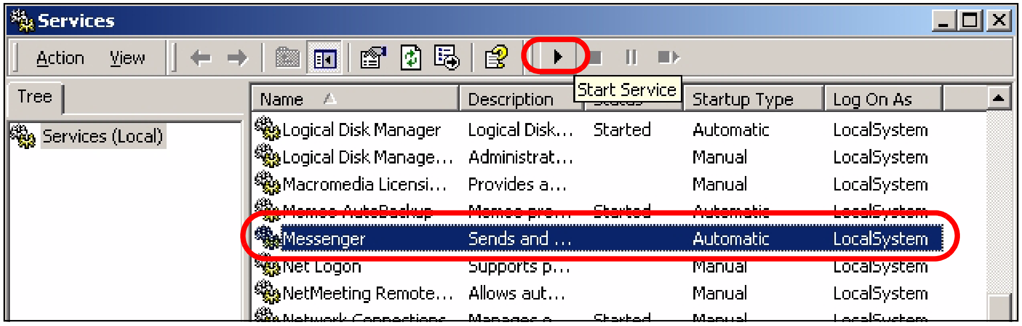
1 Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

Figure 485 Windows 2000: Opening the Services Window


My Network Places
HyperSnap-DX 5
Microsoft XML 4.0 Parser ...
iTunesSetu...
AllNetic Working Ti...
Weekly_Ba...
Recycle Bin
Adobe Photoshop ...
My Documents
Set Program Access and Defaults
Windows Update
New Office Document
Open Office Document
UltraEdit-32
SolarWinds 2003 Standard Edition
Programs
Documents
Settings
Search
Help
Run...
Shut Down...
Windows 2000 Professional
Control Panel
Network and Dial-up Connections
Printers
Taskbar & Start Menu...
Administrative Tools
Automatic Updates
Date/Time
Display
Folder Options
Fonts
Game Controllers
Intel(R) GMA Driver
Internet Options
Java
Keyboard
Mail
Mouse
Network and Dial-up Connections
Phone and Modem Options
Power Options
Printers
Regional Options
Scanners and Cameras
Scheduled Tasks
Sounds and Multimedia
System
Users and Passwords
QuickTime
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
Local Security Policy
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Performance
Server Extensions Administrator
Services
Telnet Server Administration
Start
Adobe FrameMaker (Stru...

2 Select the **Messenger** service and click **Start Service**.

Figure 486 Windows 2000: Starting the Messenger Service


Services
Action
View
Start Service
Tree
Services (Local)

Name	Description	Status	Startup Type	Log On As
Logical Disk Manager	Logical Disk…	Started	Automatic	LocalSystem
Logical Disk Manage…	Administrat…		Manual	LocalSystem
Macromedia Licensi…	Provides a…		Manual	LocalSystem
Messenger	Sends and …		Automatic	LocalSystem
Net Logon	Supports p…		Manual	LocalSystem
NetMeeting Remote…	Allows aut…		Manual	LocalSystem

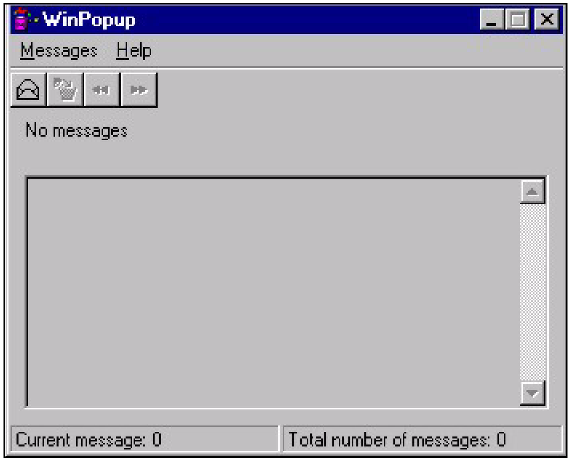
3 Close the window when you are done.

Windows 98 SE/Me

For Windows 98 SE/Me, you must open the **WinPopup** window in order to view real-time alert messages.

Click **Start** > **Run** and enter “winpopup” in the field provided and click **OK**. The **WinPopup** window displays as shown.

Figure 487 Windows 98 SE: WinPopup


WinPopup
Messages
Help

No messages

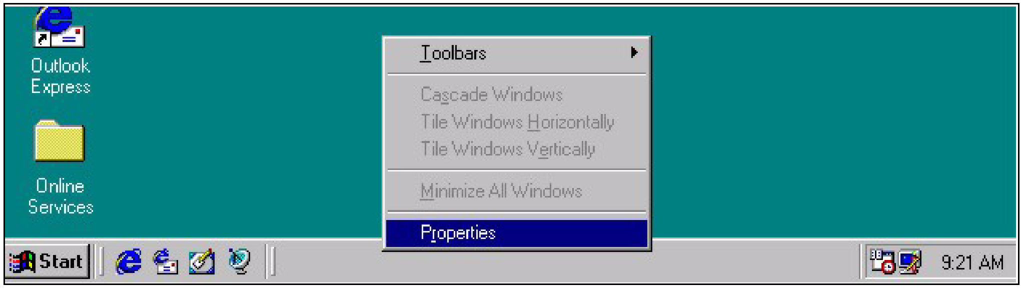
Current message: 0

Total number of messages: 0

If you want to display the WinPopup window at startup, follow the steps below for Windows 98 SE (steps are similar for Windows Me).

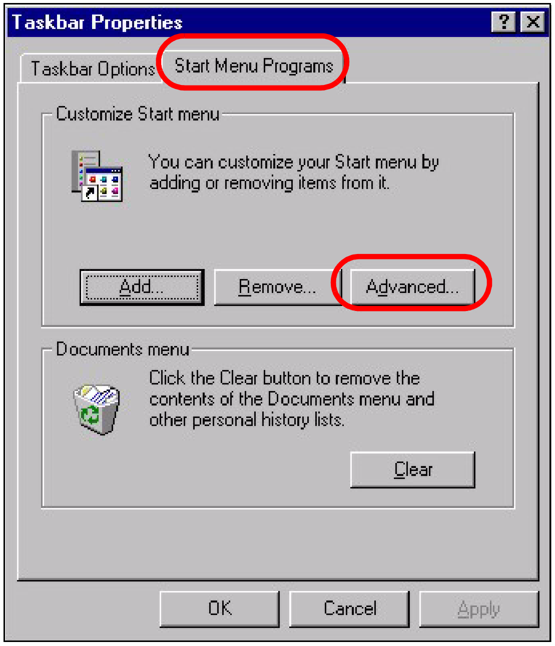
1 Right-click on the program task bar and click **Properties**.

Figure 488 WIndows 98 SE: Program Task Bar


Outlook Express
Online Services
Toolbars
Cascade Windows
Tile Windows Horizontally
Tile Windows Vertically
Minimize All Windows
Properties
Start
9:21 AM

2 Click the **Start Menu Programs** tab and click **Advanced ...**.

Figure 489 Windows 98 SE: Task Bar Properties


Taskbar Properties
Taskbar Options
Start Menu Programs
Customize Start menu
Add...
Remove...
Advanced...
Documents menu
Clear
OK
Cancel
Apply

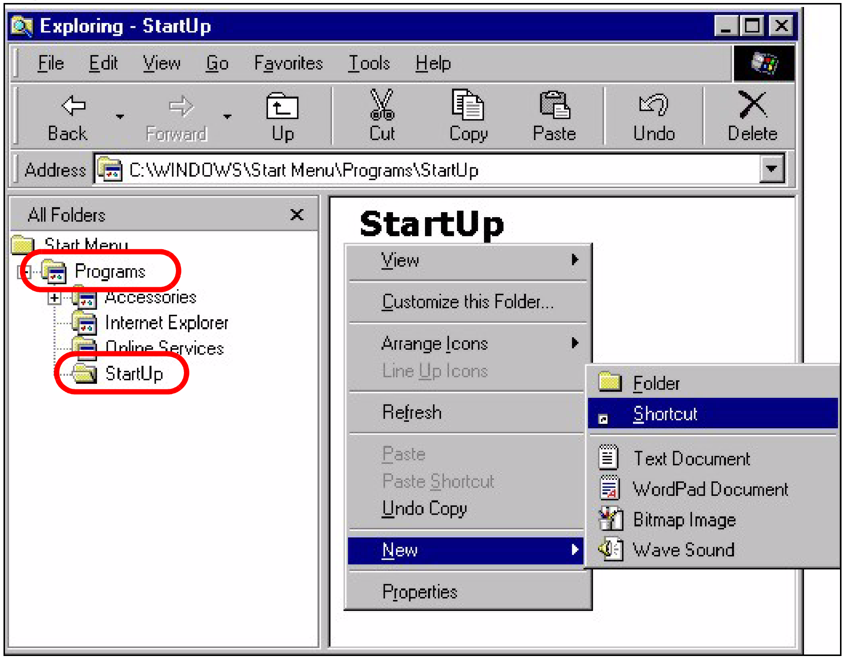
You can customize your Start menu by adding or removing items from it.

Click the Clear button to remove the contents of the Documents menu and other personal history lists.

3 Double-click **Programs** and click **StartUp**.

4 Right-click in the **StartUp** pane and click **New**, **Shortcut**.

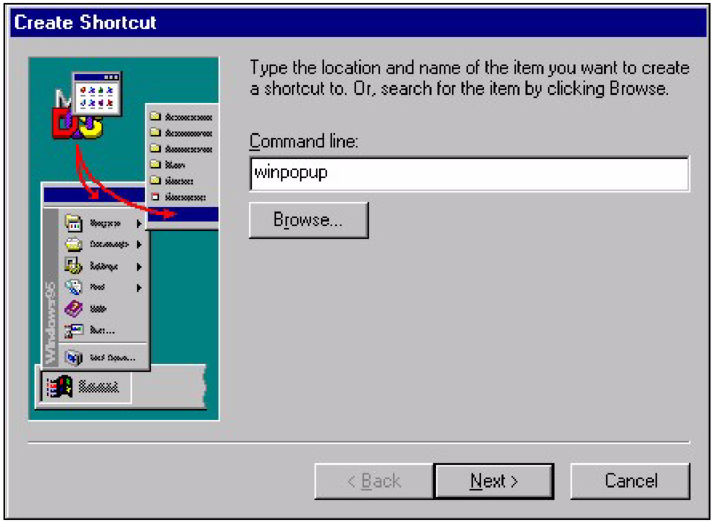
Figure 490 Windows 98 SE: StartUp


Exploring - StartUp
File
Edit
View
Go
Favorites
Tools
Help
Back
Forward
Up
Cut
Copy
Paste
Undo
Delete
Address
All Folders
Start Menu
Programs
Accessories
Internet Explorer
Online Services
StartUp
StartUp
View
Customize this Folder...
Arrange Icons
Line Up Icons
Refresh
Paste
Paste Shortcut
Undo Copy
New
Properties
Folder
Shortcut
Text Document
WordPad Document
Bitmap Image
Wave Sound

Address: C:\WINDOWS\Start Menu\Programs\StartUp

5 A **Create Shortcut** window displays. Enter “winpopup” in the **Command line** field and click **Next**.

Figure 491 Windows 98 SE: Startup: Create Shortcut



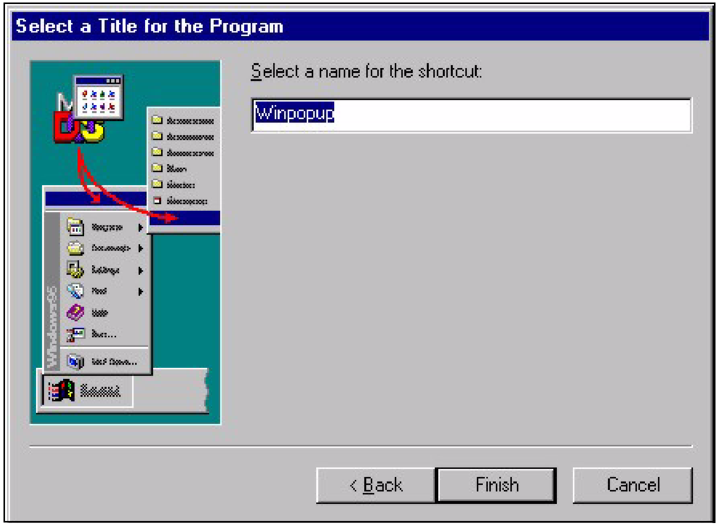
Create Shortcut

Type the location and name of the item you want to create a shortcut to. Or, search for the item by clicking Browse.

Command line: winpopup

6 Specify a name for the shortcut or accept the default and click **Finish**.

Figure 492 Windows 98 SE: Startup: Select a Title for the Program

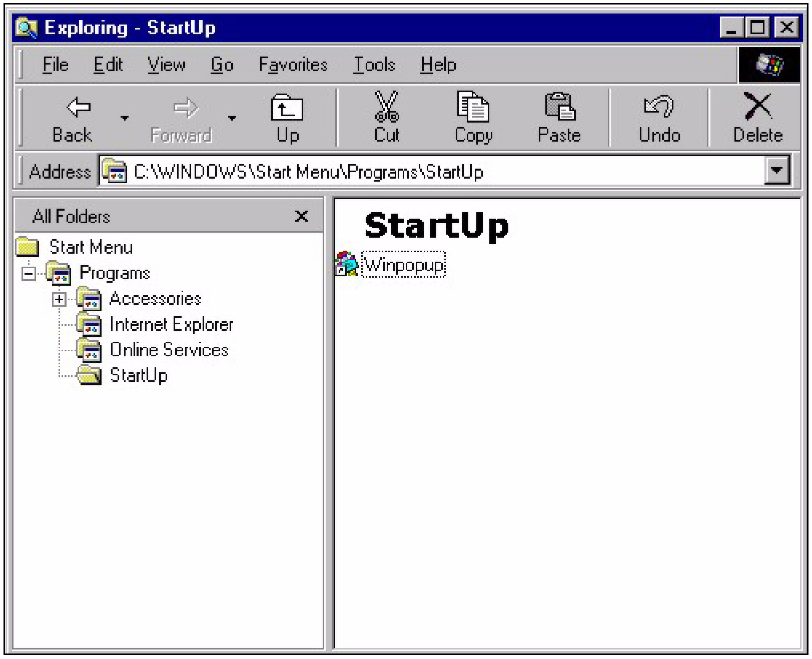


Select a Title for the Program

Select a name for the shortcut: Winpopup

7 A shortcut is created in the **StartUp** pane. Restart the computer when prompted.

Figure 493 Windows 98 SE: Startup: Shortcut


Exploring - StartUp
File
Edit
View
Go
Favorites
Tools
Help
Back
Forward
Up
Cut
Copy
Paste
Undo
Delete
Address
C:\WINDOWS\Start Menu\Programs\StartUp
All Folders
Start Menu
Programs
Accessories
Internet Explorer
Online Services
StartUp
StartUp
Winpopup

The WinPopup window displays after the computer finishes the startup process (see Figure 487 on page 709).

Importing Certificates

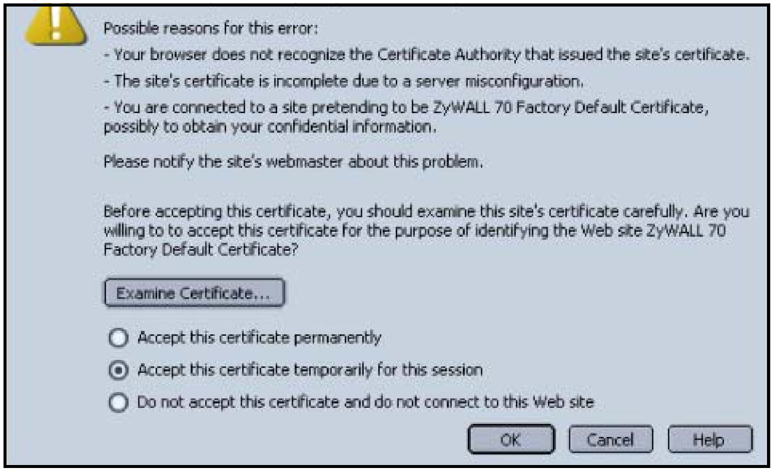
This appendix shows importing certificates examples using Netscape Navigator and Internet Explorer 5. This appendix uses the ZyWALL 70 as an example. Other models should be similiar.

Import ZyWALL Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyWALL's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

Figure 494 Security Certificate



Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site

Importing the ZyWALL's Certificate into Internet Explorer

For Internet Explorer to trust a self-signed certificate from the ZyWALL, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyWALL certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyWALL's (self-signed) server certificate into your operating system as a trusted certification authority.

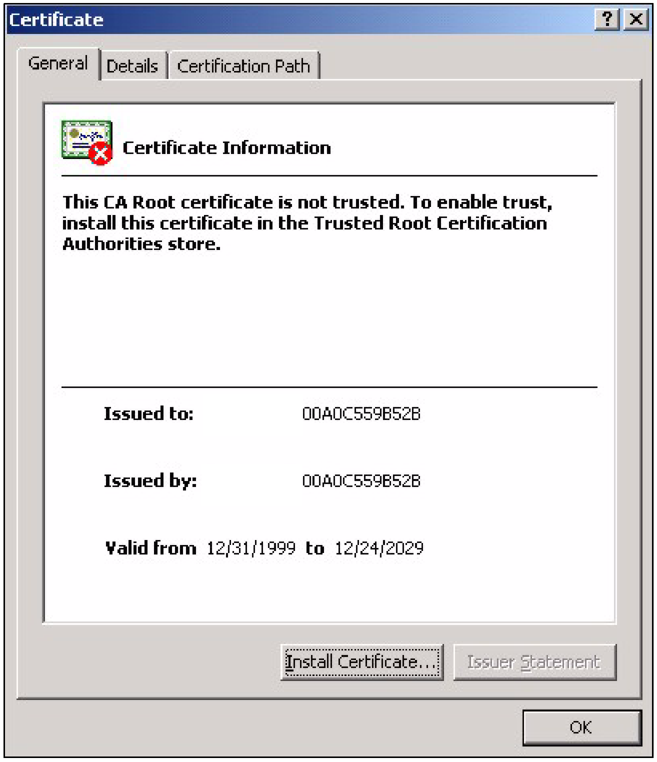
1 In Internet Explorer, double click the lock shown in the following screen.

Figure 495 Login Screen

Done
Internet

2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 496 Certificate General Information before Import


Certificate
General
Details
Certification Path
Install Certificate...
Issuer Statement
OK

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

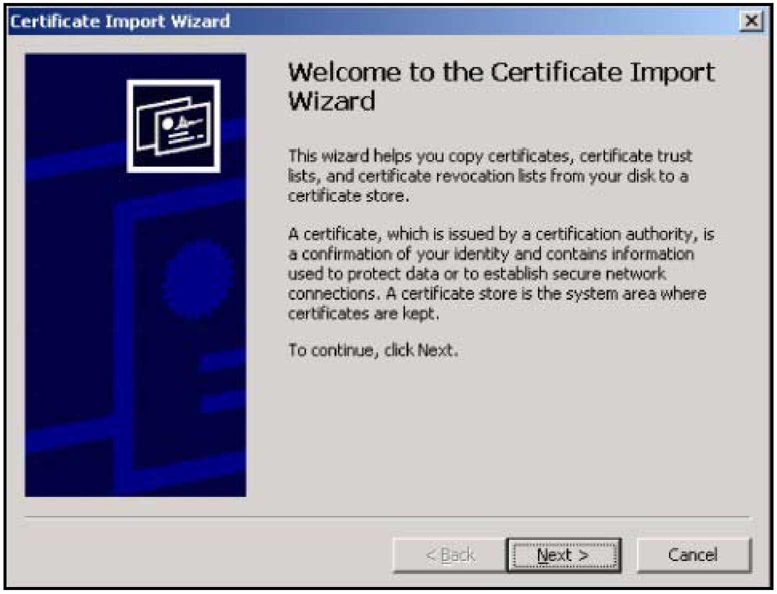
Issued to: 00A0C559B52B

Issued by: 00A0C559B52B

Valid from 12/31/1999 **to** 12/24/2029

3 Click **Next** to begin the **Install Certificate** wizard.

Figure 497 Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

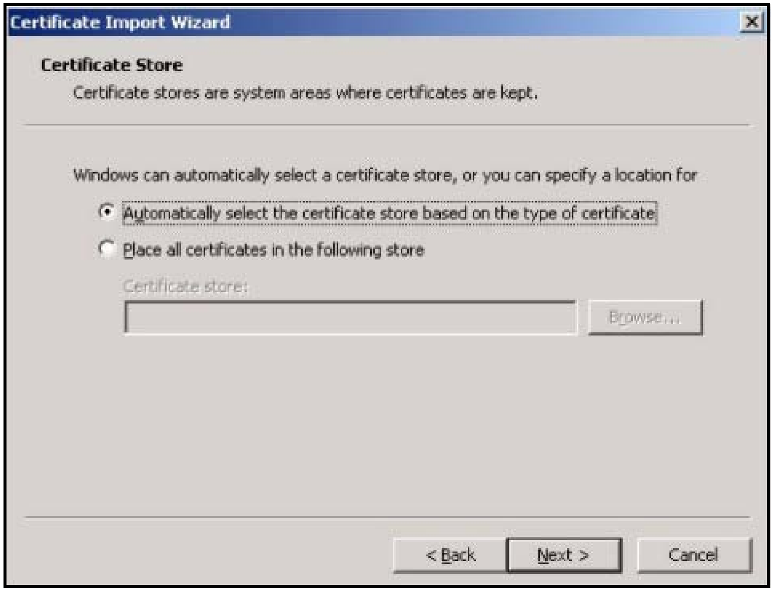
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4 Select where you would like to store the certificate and then click **Next**.

Figure 498 Certificate Import Wizard 2



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

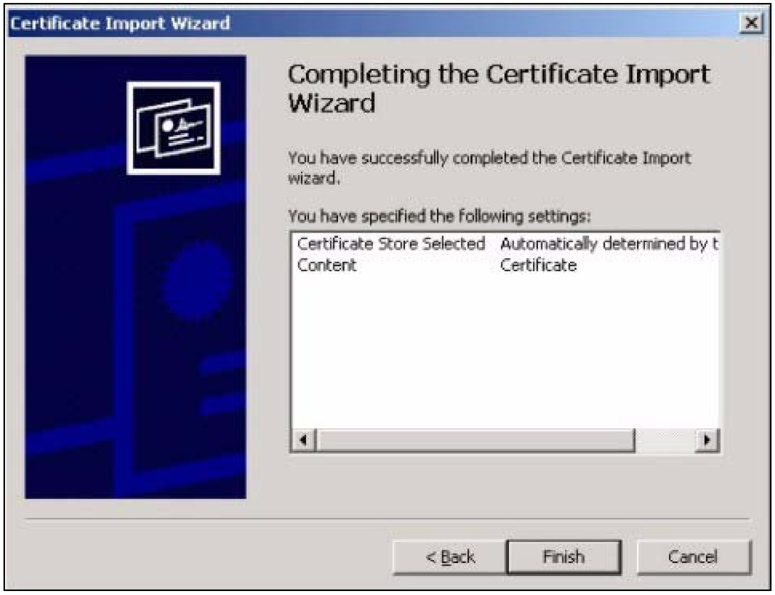
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 499 Certificate Import Wizard 3



Completing the Certificate Import Wizard

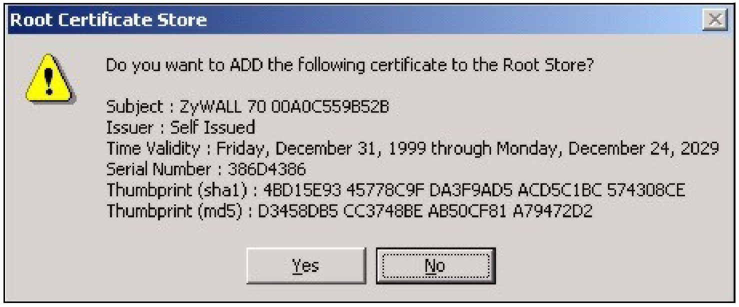
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

6 Click **Yes** to add the ZyWALL certificate to the root store.

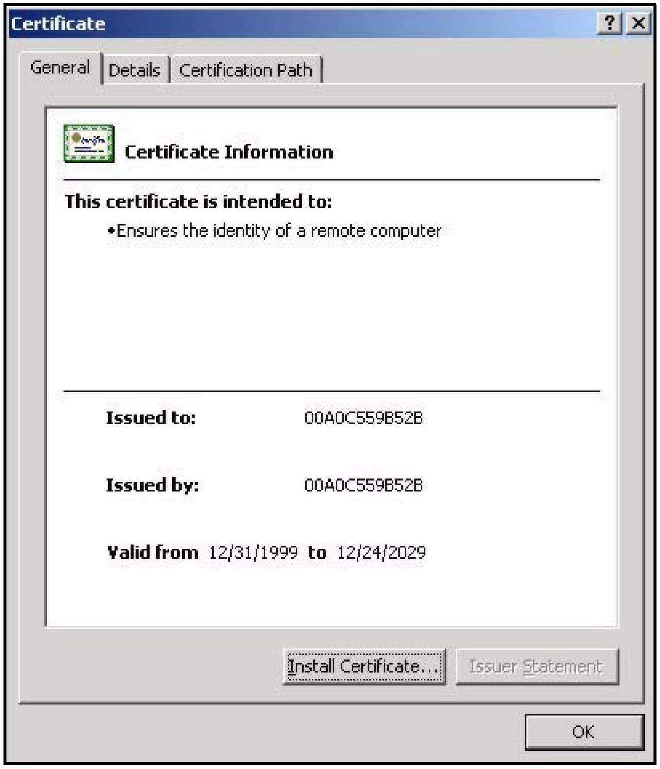
Figure 500 Root Certificate Store



Do you want to ADD the following certificate to the Root Store?

Subject : ZyWALL 70 00A0C559B52B
Issuer : Self Issued
Time Validity : Friday, December 31, 1999 through Monday, December 24, 2029
Serial Number : 386D4386
Thumbprint (sha1) : 4BD15E93 45778C9F DA3F9AD5 ACD5C1BC 574308CE
Thumbprint (md5) : D3458DB5 CC3748BE AB50CF81 A79472D2

Figure 501 Certificate General Information after Import


Certificate
?
X
General
Details
Certification Path
Install Certificate...
Issuer Statement
OK

Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: 00A0C559B52B

Issued by: 00A0C559B52B

Valid from 12/31/1999 **to** 12/24/2029

F

Open Software Announcements

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes ppp-2.4.2 software under the PPP License

PPP License

Copyright (c) 1993 The Australian National University.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the Australian National University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (c) 1989 Carnegie Mellon University.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This Product includes Netkit Telnet -0.17 software under the Netkit Telnet License

Netkit Telnet License

Copyright (c) 1989 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes ntp-4.1.2 software under the NTP License

NTP License

Copyright (c) David L. Mills 1992-2004

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

This Product includes expat-1.95.6 software under the Expat License

Expat License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This Product includes libtecla-1.6.1 software under the an X11-style License

an X11-style license

This is a Free Software License

- This license is compatible with The GNU General Public License, Version 1
- This license is compatible with The GNU General Public License, Version 2

This is just like a Simple Permissive license, but it requires that a copyright notice be maintained.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

This Product includes openssl-0.9.8d-ocf software under the OpenSSL License

OpenSSL

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This Product includes libevent-1.1a and xinetd-2.3.14 software under the a 3-clause BSD License

a 3-clause BSD-style license

This is a Free Software License

- This license is compatible with The GNU General Public License, Version 1
- This license is compatible with The GNU General Public License, Version 2

This is the BSD license without the obnoxious advertising clause. It's also known as the "modified BSD license." Note that the University of California now prefers this license to the BSD license with advertising clause, and now allows BSD itself to be used under the three-clause license.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of [original copyright holder] nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes bind-9.2.3 and dhcp-3.0.3 software under the ISC License

The ISC license for bind is:

Copyright (c) 1993-1999 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Software Consortium

950 Charter Street

Redwood City, CA 94063

Tel: 1-888-868-1001

Fax: 1-650-779-7055

Email: licensing@isc.org

This Product includes Dhcp -3.0.3 software under the DHCP License

---

The DHCP license Terms

Copyright (c) 1996-1999 Internet Software Consortium.

Use is subject to license terms which appear in the file named ISC-LICENSE that should have accompanied this file when you received it. If a file named ISC-LICENSE did not accompany this file, or you are not sure the one you have is correct, you may obtain an applicable copy of the license at:

http://www.isc.org/isc-license-1.0.html

This file is part of the ISC DHCP distribution. The documentation associated with this file is listed in the file DOCUMENTATION, included in the top-level directory of this release.

Support and other services are available for ISC products - see http://www.isc.org for more information.

This Product includes httpd-2.0.55 software developed by the Apache Software Foundation under Apache License.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

This Product includes libosip2, libgcgi-0.9.5 and p7zip_4.45/ software under LGPL license.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts

as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes bridge-utils, dhcpcd-1.3.22-pl4, rp-pppoe-3.5, vlan-1.8, keepalived-1.1.11-p1, quagga-0.99.2, ez-ipupdate-3.0.11b7, proftpd-1.2.10, libol-0.3.14, syslog-ng-1.6.5, pam-0.76, bison, tzcode2006c, iproute2, iptables-1.2.11/netfilter(kernel), dhcp-helper, busybox, Linux kernel, and pptp-linux-1.4.0 software under GPL license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND

FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes, libnet-1.1.2.1, net-snmp-5.1.1, libpcap-0.9.4, flex and openssh-4.3p2 software under BSD license

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED

AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes libxml2-2.6.8 software under the MIT License

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This Product includes openldap-2.1.10 software under the OpenLDAP License

The Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission.Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

This Product includes Folder-Tree software under the TreeView License

---

TreeView License: Distributor's License

This License For Customer Use of GubuSoft TreeView Software ("LICENSE") is the agreement which governs use of the TreeView software by GubuSoft ("GUBUSOFT") downloadable herefrom, including computer software and associated documentation ("SOFTWARE"). By downloading, installing, copying, or otherwise using the SOFTWARE, you agree to be bound by the terms of this LICENSE. If you do not agree to the terms of this LICENSE, do not use the SOFTWARE.

GUBUSOFT grants Customer a royalty-free, perpetual license to use SOFTWARE with unlimited server CPUs and internet domains. An unlimited number of end users may access and use the SOFTWARE. Customer may redistribute SOFTWARE subject to limitations. GUBUSOFT grants Customer rights to modify the source code, for use within their application.

1. DEFINITIONS

1.1 Customer. Customer means the entity or individual that downloads the SOFTWARE.

2. GRANT OF LICENSE

2.1 GUBUSOFT hereby grants Customer the following non-exclusive, non-transferable right to use the SOFTWARE.

2.1.3 LIMITATIONS

Customer may not rent, lease, or transfer the rights to the SOFTWARE to someone else.

Customer may redistribute and use SOFTWARE in source code form provided (a) Customer Applications of SOFTWARE add primary and substantial functionality, and are not merely a set or subset of any of the functionality of the SOFTWARE, or a set or subset of any of the code or other files of the SOFTWARE; (b) the source code retains all source code comments, including all copyright notices, without modification; (c) Customer includes a valid copyright notice on their Application; and (d) Customer agrees to indemnify, hold harmless, and defend GubuSoft from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of Customer's Application.

Customer may redistribute and use SOFTWARE in binary form provided (a) Customer Applications of SOFTWARE add primary and substantial functionality, and are not merely a set or subset of any of the functionality of the SOFTWARE, or a set or subset of any of the code or other files of the SOFTWARE; (b) Customer agrees to indemnify, hold harmless, and defend GubuSoft from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of Customer's Application; and (c) the following notices are included in the documentation and/or other materials provided with the Customer's Application:

Copyright (C) 2006 Conor O'Mahony (gubusoft@gubusoft.com)

All rights reserved.

This application includes the TreeView script.

You are not authorized to download and/or use the TreeView source code from this application for your own purposes. For your own FREE copy of the TreeView script, please visit the http://www.treeview.net Web site.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

If Customer is using the free version of SOFTWARE, Customer must ensure that the "JavaScript Tree Menu" link at the top of the TreeView is visible and readable in their Web page or application.

Customer may not harm the GUBUSOFT intellectual property rights using any media or via any electronic or other method now known or later discovered.

Customer may not use the GubuSoft name, the name of the TreeView author, or the names of any source code contributors to endorse or promote products derived from this SOFTWARE without specific prior written permission.

Customer may not utilize the SOFTWARE in a manner which is disparaging to GUBUSOFT.

3. TERMINATION

This LICENSE will automatically terminate if Customer fails to comply with any of the terms and conditions hereof. In such event, Customer must destroy all copies of the SOFTWARE and all of its component parts.

Defensive Suspension. If Customer commences or participates in any legal proceeding against GUBUSOFT, then GUBUSOFT may, in its sole discretion, suspend or terminate all license grants and any other rights provided under this LICENSE during the pendency of such legal proceedings.

4. COPYRIGHT

All title and copyrights in and to the SOFTWARE (including but not limited to all images, photographs, animations, video, audio, music, text, and other information incorporated into the SOFTWARE), the accompanying printed materials, and any copies of the SOFTWARE, are owned by GUBUSOFT. The SOFTWARE is protected by copyright laws and international treaty provisions. Accordingly, Customer is required to treat the SOFTWARE like any other copyrighted material, except as otherwise allowed pursuant to this LICENSE and that it may make one copy of the SOFTWARE solely for backup or archive purposes.

5. APPLICABLE LAW

This LICENSE shall be deemed to have been made in, and shall be construed pursuant to, the laws of the State of California. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

6. DISCLAIMER OF WARRANTIES AND LIMITATION ON LIABILITY

6.1 No Warranties. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS PROVIDED "AS IS" AND GUBUSOFT AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6.2 No Liability for Consequential Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL GUBUSOFT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF GUBUSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. MISCELLANEOUS

If any provision of this LICENSE is inconsistent with, or cannot be fully enforced under, the law, such provision will be construed as limited to the extent necessary to be consistent with and fully enforceable under the law. This LICENSE is the final, complete and exclusive agreement between the parties relating to the subject matter hereof, and supersedes all prior or contemporaneous understandings and agreements relating to such subject matter, whether oral or written. This LICENSE may only be modified in writing signed by an authorized officer of GUBUSOFT.

8. ASSIGNMENT

GUBUSOFT may assign or otherwise transfer any of its rights or obligations under this LICENSE agreement.

This Product includes overLIB software under the overLIB License (Artistic)

License (Artistic)

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

use the modified Package only within your corporation or organization.

rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

make other distribution arrangements with the Copyright Holder.

You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

accompany the distribution with the machine-readable source of the Package with your modifications.

accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

make other distribution arrangements with the Copyright Holder.

You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.

The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.

The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This Product includes SuperDialog software under the Creative Commons Attribution 2.5 License

Creative Commons Attribution 2.5 License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

a."Collective Work" means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

b."Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

c."Licensor" means the individual or entity that offers the Work under the terms of this License.

d."Original Author" means the individual or entity who created the Work.

e."Work" means the copyrightable work of authorship offered under the terms of this License.

f."You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights. Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a.to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b.to create and reproduce Derivative Works;

c.to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

d.to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission Derivative Works.

e.For the avoidance of doubt, where the work is a musical composition:

i.Performance Royalties Under Blanket Licenses. Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

ii.Mechanical Rights and Statutory Royalties. Licensor waives the exclusive right to collect, whether individually or via a music rights agency or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

f.Webcasting Rights and Statutory Royalties. For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4. Restrictions.The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a.You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any credit as required by clause 4(b), as requested.

b.If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

a.This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

b.Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

a.Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

b.Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

c.If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

d.No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

e.This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

NOTE: Some components of the ZyWALL incorporate source code covered under the Apache License, GPL License, LGPL License, BSD License, Open SSL License, OpenLDAP License, X11-style License, A 3 clause BSD License, NTP License, Expat License, PPP License, Netkit-telnet License, MIT License, TreeView License, overLIB's License, and Creative Commons Attribution 2.5 License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

End-User License Agreement for "ZyWALL "

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW

THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED $1,000. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

G

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

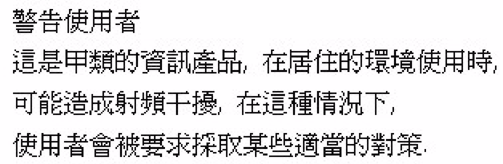
FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:



警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

H

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Numerics

3DES **308**

A

AAA servers **531**
  and authentication methods **541**
  and users **504**
  LDAP Default **533**
  LDAP Group **534**
  LDAP group members **536**
  RADIUS default **537**
  RADIUS group **538**
  RADIUS group members **539**
  RADIUS. See also RADIUS.
  where used **122**
access control **428**
access users **503**, **505**
  forcing login **505**
  forcing login. See also force user authentication policies.
  idle timeout **511**
  in user-aware policies **505**
  logging in **505**
  multiple logins **511**
  see also users **503**
  web configurator **513**
account
  myZyXEL.com **167**
action (IDP) **427**
active protocol **292**
  AH **292**
  and encapsulation **293**
  ESP **292**
active sessions. See sessions.
ActiveX **479**
AD **532**
AD (Active Directory) **531**
address groups **515**
  and content filtering **463**, **464**, **467**
  and firewall **287**
  and force user authentication policies **513**
  and FTP **606**
  and SNMP **608**
  and SSH **602**
  and Telnet **604**
  and WWW **592**
  where used **122**
address objects **515**
  and content filtering **463**, **464**, **467**
  and firewall **287**
  and force user authentication policies **513**
  and FTP **606**
  and NAT **231**
  and policy routes **230**, **231**, **513**
  and SNMP **608**
  and SSH **602**
  and Telnet **604**
  and virtual servers **258**
  and VPN connections **296**
  and WWW **592**
  HOST **515**
  RANGE **515**
  SUBNET **515**
  types of **515**
  where used **122**
admin users **503**
  multiple logins **511**
  see also users **503**
ADP
  base profiles **448**
  bindings **447**
  configuration overview **120**
  false negatives **450**
  false positives **450**
  host intrusions **445**
  inline profile **450**
  monitor profile **450**
  network intrusions **445**
  prerequisites **120**
  profiles **448**
  protocol anomaly **448**
  traffic anomaly **448**, **450**
ADP (Anomaly, Detection and Prevention) **445**
Advanced Encryption Standard. See AES.
AES **308**
AH **292**
  and transport mode **293**
alerts **627**, **628**, **631**, **634**, **635**
  anti-virus **409**
  IDP **426**
ALG **265**
  and firewall **268**
  and NAT **265**
  and policy routes **265**, **268**
  and trunks **265**

  and virtual servers 268
  FTP 265
  H.323 265, 266
  peer-to-peer calls 268
  RTP 266
  See also VoIP pass through. 265
  SIP 265, 267
  SIP timeout 268
answer rings 610
Anti-Virus
  trial service activation 167
  updating signatures 171
Anti-virus
  prerequisites 120
anti-virus 403
  alert message 707
  alerts 409
  black list 411, 413
  bypass black list 409
  bypass white list 409
  EICAR 411
  file decompression 409
  firmware package blocking 410
  log options 409
  packet scan 404, 707, 709
  priority 407
  real-time alert message 709
  registration status 407
  scanner types 404
  signatures 413
  statistics 642
  virus 403
  virus types 403
  white list 411, 412
  Windows 98/Me requirements 709
  worm 403
anti-virus scan packet types 405
Apache server 457, 458
APD
  port scanning 451
Application Layer Gateway. See ALG.
application patrol 165, 379
  actions 380
  and firewall 379
  and HTTP redirect 261
  bandwidth management 380
  bandwidth management behavior 382
  bandwidth management examples 384
  bandwidth statistics 400
  classification 379
  configuration overview 119
  configured rate effect 383
  exceptions 380
  interface's bandwidth 385
  maximize bandwidth usage 382, 383, 395, 399
  over allotment of bandwidth 384
  port-base 380
  port-less 379
  prerequisites 119
  priority 384
  priority effect 383
  protocol statistics 400
  registration status 389
  statistics 399
  unidentified applications 388
  vs firewall 278
applications 60
AppPatrol
  updating signatures 173
AppPatrol, See application patrol. 173
ASCII-encoding 457
asymmetrical routes 283
  vs virtual interfaces 283
asymmetrical routes (firewall) 284
AT command strings 609
authentication
  LDAP/AD 531
authentication algorithms 236, 307, 308
  and active protocol 307
  and routing protocols 236
  MD5 236, 308
  SHA1 308
  text 236
Authentication Header. See AH.
authentication method 532
authentication methods 541, 542
  and AAA servers 541
  and IKE SA 541
  and users 504
  and WWW 541, 592
  where used 122
authentication objects
  create 542
  example 543
Authentication, Authorization, Accounting servers. See AAA servers.
AUX port 609
auxiliary interface 179, 215, 609
  when used 215

B

backdoor 428
backup
  configuration files 618
bad-length-options 458
bandwidth
  usage statistics 400
bandwidth management 379

  and policy routes 232
  behavior 382
  configured rate effect 383
  examples 384
  in application patrol 380
  interface, outbound. See interfaces.
  interface’s bandwidth 385
  maximize bandwidth usage 227, 232, 382, 383, 384, 395, 399
  OSI level-7. See application patrol.
  over allotment of bandwidth 384
  priority 384
  priority effect 383
  See also application patrol. 379
  See also policy routes.

bare byte encoding 457

Base DN 533

base profiles 421, 448, 449

base36-encoding 457

Bind DN 533

bindings 419, 420, 447

Blaster 417, 445

bookmarks 335

boot module 621

boot sector virus 403

bridge interfaces 179, 205
  and virtual interfaces of members 205
  basic characteristics 180
  effect on routing table 205
  member interfaces 205
  virtual 217

bridges 204

buffer overflow 428

C

CA 545
  and certificates 546

Centralized Network Management
  see Vantage CNM. 610

Certificate Management Protocol (CMP) 551

Certificate Revocation List (CRL) 546
  vs OCSP 556

certificates 545
  advantages 546
  and CA 546
  and FTP 605
  and HTTPS 588
  and IKE SA 311
  and SSH 602
  and synchronization (device HA) 500
  and VPN gateways 296
  and WWW 590
  certification path 545, 553, 558
  expired 545
  factory-default 546
  file formats 546
  fingerprints 554, 560
  importing 549
  in the VPN wizard 103
  not used for encryption 545
  revoked 545
  self-signed 546, 551
  serial number 554, 559
  storage space 549, 556
  thumbprint algorithms 547
  thumbprints 547
  used for authentication 545
  verifying fingerprints 547
  where used 122

Certification Authority. See CA.

certification requests 545, 551

certifications 755
  notices 756
  viewing 756

change company logo on user screens 328

CLI 55

CLI button 72

CLI popup window 72
  display styles 73

CNM 611

cold start 55

common services 703

computer names 183, 193, 202, 209, 348

computer virus 403
  infection and prevention 403

configuration
  granularity 111

configuration example
  web-based SSL application 569

configuration files 615, 617
  at restart 617
  backup 618
  downloading 619
  downloading with FTP 605
  editing 617
  lastgood.conf 617
  managing 618
  not stopping or starting the ZyWALL 56
  startup-config.conf 617
  startup-config-bad.conf 617
  syntax 615
  system-default.conf 617
  uploading 620
  uploading with FTP 605
  use without restart 617
  way the ZyWALL runs 616

configuration information 647

connection monitor

  SSL 326
console port 55
  speed 579
content (pattern) 439
content filtering 463, 464
  and address groups 463, 464, 467
  and address objects 463, 464, 467
  and registration 466, 469
  and schedules 463, 464, 467
  and user groups 463
  and users 463
  by category 463, 468, 471
  by keyword (in URL) 463, 480
  by URL 463, 479
  by web feature 463, 479
  cache 468, 480
  categories 471
  configuration overview 120
  default policy 464, 465
  external web filtering service 468, 471
  filter list 463
  message for blocked access 465
  policies 463, 464
  prerequisites 120
  registration status 168, 466, 470
  reports. See content filtering reports.
  submitting web sites 488
  testing 476
  trial service activation 167
  uncategorized pages 471
  URL for blocked access 465
content filtering reports 483
  and registration 483
  during trial service 483
  how to look at 469, 483
content filtering reports. See also content filtering.
cookies 479
copyright 755
current date/time 158, 576
  and schedules 527
  daylight savings 577
  setting manually 579
  time server 579
current user list 326
custom signatures 432
  applying 442
  example 439
  verifying 442
custom.rules 435

D

Data Encryption Standard. See DES.
Data Terminal Ready. See DTR
daylight savings 577
DDNS 249
  backup 250
  configuration overview 117
  high availability (HA) 250
  IP address update policies 250
  mail exchanger 250
  prerequisites 117
  service providers 249
  type of service 250
  wildcard 249
default login settings 657
Default_L2TP_VPN_Connection 346
Default_L2TP_VPN_GW 346
DES 308
device HA
  configuration overview 117
  prerequisites 117
DHCP 182, 575
  and DNS servers 183
  and domain name 575
  and interfaces 182
  client list 161
  pool 182
  static DHCP 182
diagnostics 647
DIAL BACKUP port 179, 215, 609
  See also auxiliary interface.
dial-in management 609
  answer rings 610
  AT command strings 609
  Dial string 609
  DTR 609
  initial string 610
  mute 610
  port speed 610
  response strings 609
Differentiated Services Code Point (DSCP) 433
Diffie-Hellman key group 308
  Perfect Forward Secrecy (PFS) 293
directory service 532
  file structure 532
directory traversals 457
disclaimer 755
Distinguished Name (DN) 533
distributed port scans 451
DNS 580
  address records 583
  domain name forwarders 584
  domain name to IP address 583
  IP address to domain name 583
  L2TP VPN 348
  Mail eXchange (MX) records 585
  pointer (PTR) records 583
DNS servers 580, 584

- and interfaces 183
- Domain Name System. See DNS.
- double-encoding 457
- DTR 609
- Dynamic Domain Name System. See DDNS.
- Dynamic Host Configuration Protocol. See DHCP.
- DynDNS 249
  - see also DDNS.

E

- e-Donkey 427
- EGP (Exterior Gateway Protocol) 451
- EICAR 411
- e-mail virus 403
- e-Mule 427
- Encapsulating Security Payload. See ESP.
- encapsulation
  - and active protocol 293
  - transport mode 293
  - tunnel mode 293
  - VPN 293
- encryption algorithms 307, 308
  - 3DES 308
  - AES 308
  - and active protocol 307
  - DES 308
- end of IP list 434
- ESP 292
  - and transport mode 293
- Ethereal 440
- Ethernet interfaces 179, 184
  - and OSPF 185
  - and RIP 185
  - and routing protocols 185
  - basic characteristics 180
  - virtual 217
  - with no physical ports 195
- experimental-options 458
- extended authentication
  - and VPN gateways 296
  - IKE SA 311
- external modems 215

F

- false negatives 423, 450
- false positives 423, 450, 456
- FCC interference statement 755
- feature specifications 657
- file decompression
  - anti-virus 409
- file extensions
  - configuration files 615
  - shell scripts 615
- file infector 403
- file manager
  - configuration overview 124
- file sharing SSL application 567
  - create 570
- filtered port scan 452
- firewall 57, 277
  - actions 287
  - and address groups 287
  - and address objects 287
  - and alerts 282
  - and ALG 268
  - and application patrol 379
  - and H.323 (ALG) 266
  - and HTTP redirect 261
  - and IPSec SA 280
  - and IPSec VPN 297
  - and logs 287
  - and port triggering 226
  - and schedules 287, 394, 396, 398
  - and service groups 287
  - and services 287, 522
  - and SIP (ALG) 267
  - and user groups 287
  - and users 287
  - and virtual servers 279
  - and VoIP pass through 265, 268
  - and zones 277, 285
  - asymmetrical routes 284
  - configuration overview 118
  - criteria 278
  - global rules 279
  - prerequisites 118
  - priority 285
  - sessions, number of 285
  - to-ZyWALL. See also to-ZyWALL firewall.
  - triangle routes 284
  - vs application patrol 278
- firmware
  - and restart 620
  - boot module. See boot module.
  - current version 158, 621
  - getting updated 620
  - uploading 620, 621
  - uploading with FTP 605
- flags 433
- flood detection 452
- force log out 327
- force user authentication policies 511
  - and address groups 513

  and address objects 513
  and schedules 513
  prerequisites 123
fragmentation flag 437
fragmentation offset 437
FTP 605
  additional signaling port 270
  and address groups 606
  and address objects 606
  and certificates 605
  and zones 605
  signaling port 270
  with Transport Layer Security (TLS) 605
full tunnel mode 61
full-tunnel mode 326
Fully-Qualified Domain Name (FQDN) 583

G

gateway policy. See VPN gateways.
Generic Routing Encapsulation. See GRE.
global SSL setting 327
  user portal logo 328
GRE 211

H

H.323 266
  additional signaling port 270
  and firewall 266
  and RTP 266
  signaling port 270
H.323. See also ALG.
header checksum 433
host-based intrusions 417, 445
HTTP
  redirect to HTTPS 590
  vs HTTPS 588
HTTP Inspection 457
HTTP over SSL. See HTTPS.
HTTP redirect 261
  and application patrol 261
  and firewall 261
  and interfaces 264
  and policy routes 261
  configuration overview 121
  packet flow 261
  prerequisites 121
HTTPS 588
  and certificates 588
  authenticating clients 588
  avoiding warning messages 594
  example 592
  vs HTTP 588
  with Internet Explorer 593
  with Netscape Navigator 593
hub-and-spoke VPN. See VPN concentrator.
HyperText Transfer Protocol over Secure Socket Layer. See HTTPS.

I

ICMP 521
ICMP code 438
ICMP Decoder 457
ICMP echo 452
ICMP flood 452
ICMP portsweep 451
ICMP sequence number 438
ICMP type 438
ICMP unreachable 452
identification (IP) 437
IDP
  action 427
  alerts 426
  and services 522
  applying custom signatures 442
  base profiles 421
  bindings 419, 420
  configuration overview 120
  custom signature example 439
  custom signatures 432
  false negatives 423
  false positives 423
  inline profile 423
  license status 158, 159
  log options 426
  packet inspection profiles 424
  packet inspection signatures
    signatures
      packet inspection 424
  policy types 427
  prerequisites 120
  profiles 418, 419
  query view 426, 429
  registration status 168, 420
  reject sender 427
  reject-both 427
  reject-receiver 427
  severity 426
  signature ID 426
  signatures
    signatures

  - IDP 418
  - Snort signatures 443
  - statistics 643
  - traffic directions 418
  - updating signatures 173
  - verifying custom signatures 442
- IDP (Intrusion, Detection and Prevention) 417
- IDP and AppPatrol
  - trial service activation 167
- IDP profiles 421
- IDP service group 428
- IDP signature categories 427
- IDP signatures
  - and synchronization (device HA) 500
- IEEE 802.1q. See VLAN.
- IGP (Interior Gateway Protocol) 451
- IHL (IP Header Length) 433
- IIS server 457
- IIS unicode 457
- IKE SA
  - aggressive mode 307, 310
  - and authentication methods 541
  - and certificates 311
  - and RADIUS 311
  - and to-ZyWALL firewall 297
  - authentication algorithms 307, 308
  - configuration overview 116
  - content 309
  - dead peer detection (DPD) 315
  - Diffie-Hellman key group 308
  - encryption algorithms 307, 308
  - extended authentication 311
  - ID type 309
  - IP address, remote IPSec router 307
  - IP address, ZyXEL device 307
  - local identity 309
  - main mode 307, 310
  - NAT traversal 311
  - negotiation mode 307
  - password 311
  - peer identity 309
  - prerequisites 116
  - pre-shared key 309
  - proposal 307
  - user name 311
- IKE SA. See also VPN.
- initial string 610
- inline profile 423, 450
- instant messenger (IM)
  - managing 165, 379
- interface
  - bandwidth 385
  - status 159, 186
- interfaces
  - and DNS servers 183
  - and HTTP redirect 264
  - and layer-3 virtualization 179
  - and physical ports 112, 179
  - and policy routes 230, 231
  - and static routes 234
  - and virtual servers 258
  - and VPN gateways 296
  - and VRRP groups 495
  - and zones 112, 179
  - as DHCP relays 182
  - as DHCP servers 182, 575
  - auxiliary. See also auxiliary interface.
  - backup. See trunks.
  - bandwidth management 182, 223
  - bridge. See also bridge interfaces.
  - configuration overview 115
  - DHCP clients 181
  - Ethernet. See also Ethernet interfaces.
  - gateway 181
  - general characteristics 179
  - IP address 180
  - metric 181
  - MTU 182
  - overlapping IP address and subnet mask 181
  - ping check 183
  - port groups. See also port groups.
  - PPPoE/PPTP. See also PPPoE/PPTP interfaces.
  - prerequisites 115, 184
  - relationships between 184
  - static DHCP 182
  - subnet mask 180
  - trunks. See also trunks.
  - types 179
  - virtual. See also virtual interfaces.
  - VLAN. See also VLAN interfaces.
  - where used 115
- Internet Control Message Protocol. See ICMP.
- Internet Protocol Security. See IPSec.
- Internet Protocol. See IP.
- intrusions
  - host 417, 445
  - network 417, 445
- IP 432
- IP alias. See virtual interfaces.
- IP decoy portscan 451
- IP distributed portscan 451
- IP options 434, 438
- IP policy routing. See policy routes.
- IP pool 326
- IP portscan 451
- IP portsweep 451
- IP protocols 521
  - ICMP. See ICMP.
  - TCP. See TCP.
  - UDP. See UDP.
- IP security option 434

IP static routes. See static routes.
IP stream identifier 434
IP v4 packet headers 433
IPSec 291
  basic troubleshooting 297
  connections 296
  Default_L2TP_VPN_Connection 346
  Default_L2TP_VPN_Connection example 353
  Default_L2TP_VPN_GW 346
  Default_L2TP_VPN_GW example 351
  established in two phases 291
  L2TP VPN 345
  local network 291
  remote IPSec router 291
  remote network 291
  SA 292
  SA monitor 320
  See also VPN.
IPSec SA
  active protocol 292
  and firewall 280, 297
  and to-ZyWALL firewall 297
  authentication algorithms 307, 308
  authentication key (manual keys) 294
  configuration overview 116
  destination NAT for inbound traffic 296
  encapsulation 293
  encryption algorithms 307, 308
  encryption key (manual keys) 294
  local policy 292
  manual keys 294
  NAT for inbound traffic 294
  NAT for outbound traffic 294
  overlapping policies 305
  Perfect Forward Secrecy (PFS) 293
  policy enforcement 301
  prerequisites 116
  proposal 293
  remote policy 292
  search by name 321
  search by policy 321
  Security Parameter Index (SPI) (manual keys) 294
  source NAT for inbound traffic 295
  source NAT for outbound traffic 295
  status 320
  transport mode 293
  tunnel mode 293
  when IKE SA is disconnected 292
  where used 116
IPSec SA. See also VPN.
ISP accounts 563
  and PPPoE/PPTP interfaces 211, 563
  authentication type 565
  encryption method 565
  stac compression 565

J

Java 479

K

kick out user 327
kill user session 327

L

L2TP VPN 345
  configuring in Windows 2000 361
  configuring in Windows XP 356
  Default_L2TP_VPN_Connection 346
  Default_L2TP_VPN_Connection example 353
  Default_L2TP_VPN_GW 346
  Default_L2TP_VPN_GW example 351
  DNS 348
  example 351, 354
  IPSec configuration 345
  policy route 346
  policy route example 354
  remote user configuration 355
  session monitor 348
  WINS 348
LAND attack 453
lastgood.conf 617
Layer 2 Tunneling Protocol Virtual Private Network, See L2TP VPN. 345
LDAP 532
  and users 504
  CN identifier 534
  user attributes 504
LDAP (Lightweight Directory Access Protocol) 531
LDAP directory structure 532
least load first (for load balancing) 220
license key 169
load balancing 219
  algorithms 220, 223
  least load first 220
  session-oriented 220
  spillover 221
  weighted round robin 221
load balancing. See also trunks.
local user database 531
log messages 627
  categories 631, 634, 635
  debugging 625
  regular 625

  types of 625
log options 409
log options (IDP) 426
logged in users 163
login
  default settings 657
  SSL user 332
logo 328
logout
  SSL user 335
logs
  and firewall 287
  configuration overview 124
  descriptions 663
  e-mail profiles 627
  e-mailing log messages 626, 631
  formats 628
  log consolidation 632
  specifications 625
  syslog servers 627
  system 627
  types of 627
loose source routing 434

M

MAC addresses
  and VLAN 197
  ZyWALL 158
macro virus 403
Management Information Base (MIB) 607
MD5 308
Message Digest 5. See MD5.
metrics. See reports.
model name 158
monitor 326
monitor profile 450
  IDP
    monitor profile 423
MS-05-39 439
multiple slash encoding 457
mute 610
My Certificates. See also certificates. 548
MyDoom 417, 445
myZyXEL.com 165, 173
  accounts, creating 165
  and IDP 420
myZyXEL.com account 167

N

NAT 226, 256
  1
    1 example 147
  address mapping. See policy routes.
  ALG. See ALG.
  and address objects 231
  and ALG 265
  and policy routes 225, 231
  and VPN 311
  and VPN. See also VPN.
  port forwarding. See virtual servers.
  port translation. See virtual servers.
  port triggering. See also policy routes.
  port triggering. See also port triggering.
  trigger port. See also policy routes.
NAT traversal 311
NBNS 183, 193, 202, 209, 326
  L2TP VPN 348
NetBIOS Name Server. See NBNS.
NetMeeting. See H.323.
network access mode 60
  full tunnel 61
  reverse proxy 60
Network Address Translation. See NAT.
network list
  SSL 326
network policy. See VPN connections.
Network Time Protocol (NTP) 578
network-based intrusions 417, 445
Nimda 417, 445
Nmap 451
no IP options 434
non-RFC characters 457
non-rfc-http-delimiter 457

O

object 323
  SSL application 567
objects 122
obsolete-options 458
offset (patterns) 439
Online Certificate Status Protocol (OCSP) 556
  vs CRL 556
Open Shortest Path First. See OSPF.
original setting (IDP) 426
OSI (Open System Interconnection) 421
OSPF 237
  and Ethernet interfaces 185

  and RIP 239
  and static routes 239
  and to-ZyWALL firewall 238
  area 0 239
  areas. See OSPF areas.
  authentication method 185
  autonomous system (AS) 237
  backbone 239
  Configuration steps 240
  direction 185
  link cost 185
  priority 185
  redistribute 239
  redistribute type (cost) 242
  routers. See OSPF routers.
  virtual links 240
  vs RIP 235

OSPF areas 238
  and Ethernet interfaces 185
  backbone 238
  Not So Stubby Area (NSSA) 238
  stub areas 238
  types of 238

OSPF routers 239
  area border (ABR) 239
  autonomous system boundary (ASBR) 239
  backbone (BR) 239
  backup designated (BDR) 240
  designated (DR) 240
  internal (IR) 239
  link state advertisements
  priority 240
  types of 239

oversize-chunk-encoding 458

oversize-offset 458

oversize-request-uri-directory 458

P

packet inspection
  signatures 424

packet inspection signatures 421

packet scan 404, 709

packet statistics 162

padding 434

payload option 438

payload size 439

peer-to-peer (P2P)
  managing 165, 379

peer-to-peer calls 268

Perfect Forward Secrecy (PFS)
  Diffie-Hellman key group 293

physical port
  packet statistics 162

physical ports 113
  and interfaces 112

ping check. See interfaces.

Point-to-Point Protocol over Ethernet. See PPPoE.

Point-to-Point Tunneling Protocol. See PPTP

policy route
  L2TP VPN 346
  L2TP VPN example 354

policy routes 225
  actions 225
  and address objects 230, 231, 513
  and ALG 265, 268
  and HTTP redirect 261
  and interfaces 230, 231
  and NAT 225
  and schedules 230, 392, 394, 396, 398
  and service groups 230
  and services 230, 522
  and trunks 219, 231
  and user groups 230, 392, 394, 396, 398
  and users 230, 392, 394, 396, 398
  and VoIP pass through 268
  and VPN connections 230, 231, 296
  bandwidth management 232
  benefits 225
  configuration overview 117
  criteria 225
  prerequisites 117

port forwarding. See virtual servers.

port groups 179, 194, 195
  and Ethernet interfaces 194
  and physical ports 194
  representative interfaces 195

port scanning 451

port speed 610

port sweep 451

port translation. See virtual servers.

port triggering 226
  and firewall 226
  and policy routes 231
  and service groups 231
  and services 231

power off 55

power on 55

PPPoE 210, 211
  and RADIUS 211
  TCP port 1723 211

PPPoE/PPTP interfaces 179, 211
  and ISP accounts 211, 563
  basic characteristics 180
  gateway 211
  subnet mask 181, 211

PPTP 210
  and GRE 211

  - as VPN **211**
- product registration **757**
- profiles
  - ADP **448**
  - packet inspection **424**
- protocol
  - usage statistics **400**
- protocol anomaly **448**, **457**
- protocol anomaly detection **457**
- proxy servers **261**
  - web. See web proxy servers.
- Public-Key Infrastructure (PKI) **546**
- public-private key pairs **545**

Q

- query view (IDP) **426**, **429**
- Quick Start Guide **65**

R

- RADIUS **531**, **536**
  - advantages **536**
  - and IKE SA **311**
  - and PPPoE **211**
  - and users **504**
  - user attributes **505**
- real-time alert message **709**
- Real-time Transport Protocol. See RTP.
- reboot **55**, **649**
  - vs reset **649**, **652**
- record route **434**
- registration
  - and content filtering **466**, **469**
  - configuration overview **124**
  - prerequisites **124**
  - product **757**
  - subscription services. See subscription services.
- registration status
  - anti-virus **407**
  - application patrol **389**
  - IDP **420**
- reject-both (IDP) **427**
- reject-receiver (IDP) **427**
- reject-sender (IDP) **427**
- related documentation **3**
- Remote Authentication Dial-In User Service. See RADIUS.
- remote management
  - and users **588**
  - CNM **611**
  - configuration overview **123**
  - FTP. See FTP.
  - prerequisites **123**
  - Telnet **604**
  - timeouts **588**
  - to-ZyWALL firewall **279**
  - WWW. See WWW.
- remote management connection **609**
- remote management, see service control **587**
- remote user screen links **567**
- reports
  - anti-virus **642**
  - collecting data **637**
  - configuration overview **124**
  - IDP **643**
  - specifications **640**
  - types of **637**
- reset **652**
  - vs reboot **649**, **652**
- RESET button **55**, **652**
- response strings **609**
- reverse proxy mode **60**
- RFC 1058. See RIP.
- RFC 1389. See RIP.
- RFC 1587. See OSPF areas.
- RFC 1631. See NAT.
- RFC 1889. See RTP.
- RFC 2131. See DHCP.
- RFC 2132. See DHCP.
- RFC 2328. See OSPF.
- RFC 2338. See VRRP.
- RFC 2402. See AH.
- RFC 2406. See ESP.
- RFC 2510. See Certificate Management Protocol.
- RFC 2516. See PPPoE.
- RFC 2637. See PPTP.
- RFC 2890. See GRE.
- RFC 3261. See SIP.
- RIP **235**
  - and Ethernet interfaces **185**
  - and OSPF **235**
  - and static routes **235**
  - and to-ZyWALL firewall **236**
  - authentication **235**
  - direction **185**
  - redistribute **235**
  - RIP-2 broadcasting methods **185**
  - versions **185**
  - vs OSPF **235**
- round robin (for load balancing) **221**
- Routing Information Protocol. See RIP
- routing protocols **235**

  and authentication algorithms 236
  and Ethernet interfaces 185
RTP 266
  See also ALG. 266

S

safety warnings 7
same IP 438
scanner types 404
schedules 527
  and content filtering 463, 464, 467
  and current date/time 527
  and firewall 287, 394, 396, 398
  and force user authentication policies 513
  and policy routes 230, 392, 394, 396, 398
  one-time 527
  recurring 527
  types of 527
  where used 122
Secure Hash Algorithm. See SHA1.
Secure Socket Layer. See SSL.
security associations. See VPN.
self-referential directories 458
sensitivity level 456
serial number 158
service control 587
  and to-ZyWALL firewall 587
  limitations 588
service groups 522
  and firewall 287
  and policy routes 230
  and port triggering 231
  where used 122
services 521, 703
  and firewall 287, 522
  and IDP 522
  and policy routes 230, 522
  and port triggering 231
  where used 122
Session Initiation Protocol. See SIP.
session monitor
  L2TP VPN 348
sessions 640
severity (IDP) 422, 426
SHA1 308
shell scripts 615
  and users 505
  downloading 623
  editing 622
  managing 622
  not stopping or starting the ZyWALL 56
  syntax 615
  uploading 624
  way the ZyWALL runs 616
shutdown 55
signature categories
  access control 428
  buffer overflow 428
  DoS/DDoS 428
  IM 427
  P2P 427
  scan 428
  spam 427
  virus/worm 428
  Web attack 428
signature ID 426, 435, 437
signatures
  anti-virus 413
Simple Certificate Enrollment Protocol (SCEP) 551
Simple Network Management Protocol. See SNMP.
Simple Traversal of UDP through NAT. See STUN.
SIP 267
  additional signaling port 270
  and firewall 267
  and RTP 266
  media inactivity timeout 270
  signaling inactivity timeout 270
  signaling port 270
smurf attack 452
SNAT 226
SNMP 606, 607
  agents 607
  and address groups 608
  and address objects 608
  and zones 608
  Get 607
  GetNext 607
  Manager 607
  managers 607
  MIB 607
  network components 606
  Set 607
  Trap 607
  traps 607
  versions 606
Snort equivalent terms 443
Snort rule header 443
Snort rule options 443
Snort signatures 443
Source Network Address Translation. See SNAT.
specifications 657
  device 657
  feature 657
  hardware 657
spillover (for load balancing) 221
SQL slammer 417, 445

SSH **600**
  and address groups **602**
  and address objects **602**
  and certificates **602**
  and zones **602**
  client requirements **601**
  encryption methods **601**
  for secure Telnet **602**
  how connection is established **600**
  versions **601**
  with Linux **603**
  with Microsoft Windows **602**

SSL **326**, **588**
  certificates **332**
  computer names **326**
  full-tunnel mode **326**
  global setting **327**
  IP pool **326**
  monitor **326**
  network list **326**
  policy **323**
  remote user login **332**
  remote user logout **335**
  user screen bookmarks **335**
  user screens **331**, **334**
  user screens access methods **331**
  user screens certificates **332**
  user screens login **332**
  user screens logout **335**
  user screens required information **332**
  user screens system requirements **331**
  WINS **326**

SSL application
  edit **568**

SSL application object **567**
  add **568**
  file sharing **567**
  file sharing application **570**
  remote user screen links **567**
  summary **567**
  types **567**
  web-based **567**, **568**
  web-based example **569**

SSL connection monitor **326**

SSL policy **323**
  add **325**
  edit **325**
  objects used **323**

stac compression **565**

starting the ZyWALL **55**

startup-config.conf **617**
  and synchronization (device HA) **500**
  if errors **617**
  missing at restart **617**
  present at restart **617**

startup-config-bad.conf **617**

static routes **232**
  and interfaces **234**
  and OSPF **239**
  and RIP **235**
  configuration overview **118**
  metric **234**
  prerequisites **118**

statistics
  anti-virus **642**
  application patrol **399**
  bandwidth **400**
  IDP **643**
  protocol **400**

status bar **72**
  warning message popup **72**

stopping the ZyWALL **55**

streaming protocols
  managing **165**, **379**

strict source routing **434**

STUN
  and VoIP pass through **265**

subscription services **165**
  and synchronization (device HA) **500**
  AppPatrol **165**
  content filtering **166**
  content filtering. See also content filtering.
  IDP **165**
  IDP. See also IDP.
  new IDP or AppPatrol signatures **166**
  SSL VPN **166**
  SSL VPN. See also SSL VPN.
  status **168**, **389**, **407**
  trial service activation **167**
  upgrading **169**

Supporting Disk **4**

SYN flood **453**

synchronization **500**
  and subscription services **500**
  information synchronized **500**
  password **501**
  port number **501**
  restrictions **500**

syntax conventions **5**

syslog servers. See logs.

system log. See logs.

system name **158**

system protect
  updating signatures **175**

system reports. See reports.

system uptime **158**

system-default.conf **617**

T

T/TCP 458
task bar properties 710
TCP 521
  ACK (acknowledgment) 453
  ACK number 438
  connections 521
  port numbers 521
  SYN (synchronize) 453
  window size 438
TCP Decoder 457
TCP decoy portscan 451
TCP distributed portscan 451
TCP flag bits 438
TCP portscan 451
TCP portsweep 451
TCP RST 452
TCP SYN flood 453
TCPdump 440
Telnet 604
  and address groups 604
  and address objects 604
  and zones 604
  with SSH 602
terminate user connection 327
terminology differences
  bandwidth management 112
  NAT 112
  with other products 112
  with ZyNOS 112
three-way handshake 453
through-ZyWALL firewall. See firewall.
time servers (default) 578
time to live 433
timestamp 434
to-ZyWALL firewall 279
  and NAT traversal (VPN) 297
  and OSPF 238
  and remote management 279
  and RIP 236
  and service control 587
  and virtual servers 256
  and VPN 297
  and VRRP 495
  and VRRP groups 495
  global rules 279
to-ZyWALL firewall. See also firewall.
trademarks 755
traffic anomaly 448, 450
Transmission Control Protocol. See TCP.
Transport Layer Security (TLS) 605
trial subscription services 167
triangle routes 283
  vs virtual interfaces 283
triangle routes (firewall) 284
Triple Data Encryption Standard. See 3DES.
troubleshooting 647, 651
truncated-address-header 459
truncated-header 459
truncated-options 458
truncated-timestamp-header 459
trunks 180, 219
  and ALG 265
  and policy routes 219, 231
  configuration overview 115
  member interface mode 223
  member interfaces 223
  prerequisites 116
  where used 116
trunks. See also load balancing.
Trusted Certificates. See also certificates. 556

U

u encoding 458
UDP 521
  messages 521
  port numbers 521
UDP Decoder 457
UDP decoy portscan 451
UDP distributed portscan 451
UDP flood attack 454
UDP portscan 451
UDP portsweep 451
undersize-len 458
undersize-offset 458
updating
  Anti-Virus signatures 171
  IDP and AppPatrol signatures 173
  system protect signatures 175
upgrading license 169
URI (Uniform Resource Identifier) 439
usage
  CPU 158
  flash 158
  memory 158
  onboard flash 158
  sessions 158
user authentication 503, 531, 532
  external 504
  local user database 531
User Datagram Protocol. See UDP.
user groups 505

  and content filtering 463
  and firewall 287
  and policy routes 230, 392, 394, 396, 398
  configuration overview 122
user names
  rules 508
user portal
  See SSL user screens. 331, 334
user portal links 567
user portal logo 328
user sessions. See sessions.
user SSL screens 331, 334
  access methods 331
  bookmarks 335
  certificates 332
  login 332
  logout 335
  required information 332
  system requirements 331
users 503
  access. See also access users.
  Admin (type) 503
  admin. See also admin users.
  and AAA servers 504
  and authentication methods 504
  and content filtering 463
  and firewall 287
  and LDAP 504
  and policy routes 230, 392, 394, 396, 398
  and RADIUS 504
  and remote management 588
  and shell scripts 505
  attributes for Ext-User 504
  attributes for LDAP 504
  attributes for RADIUS 505
  attributes in AAA servers 504
  configuration overview 122
  currently logged in 158, 163
  default lease time 510
  default reauthentication time 510
  default type for Ext-User 504
  Ext-User (type) 503, 504
  groups. See user groups.
  Guest (type) 503
  lease time 507
  Limited-Admin (type) 503
  lockout 511
  prerequisites (for force user authentication policies) 123
  reauthentication time 507
  types of 503
  User (type) 503
  user names 508
UTF-8 decode 458

V

Vantage CNM 610
virtual interfaces 179, 217
  basic characteristics 180
  not DHCP clients 181
  types of 217
  vs asymmetrical routes 283
  vs triangle routes 283
Virtual Local Area Network. See VLAN.
Virtual Private Network. See VPN.
Virtual Router Redundancy Protocol. See VRRP.
virtual servers 255
  and address objects (HOST) 258
  and ALG 268
  and firewall 279
  and interfaces 258
  and to-ZyWALL firewall 256
  and VoIP pass through 268
  configuration overview 121
  criteria 255
  limitations 226
  prerequisites 121
  where to forward 255
virus 428
virus attack 403
virus life cycle 403
virus scan 404
VLAN 196
  advantages 197
  and MAC addresses 197
  ID 197
VLAN interfaces 179, 198
  and Ethernet interfaces 198
  basic characteristics 180
  virtual 217
VoIP pass through 266
  and firewall 265, 268
  and policy routes 268
  and virtual servers 268
  configuration overview 122
  peer-to-peer calls 268
VoIP pass through. See also ALG. 265
VPN 291
  active protocol 292
  and NAT 311
  basic troubleshooting 297
  hub-and-spoke. See VPN concentrator.
  IKE SA. See IKE SA.
  IPSec 291
  IPSec SA. See IPSec SA.
  proposal 307
  security associations (SA) 291
  status 160
VPN concentrator 318

  advantages 318
  and IPSec SA policy enforcement 320
  disadvantages 318
VPN connections
  and address objects 296
  and policy routes 230, 231, 296
VPN gateways
  and certificates 296
  and extended authentication 296
  and interfaces 296
  and to-ZyWALL firewall 297
VPN. See also IKE SA, IPSec SA.
VRRP 493
  advertisement interval 493
  and to-ZyWALL firewall 495
  backup router 493
  management IP 493
  master router 493
  preempt 494
  router priority 494
  virtual router ID (VR ID) 493
VRRP groups 495
  advertisement interval 495
  and interfaces 495
  and to-ZyWALL firewall 495
  authentication 495
  HA status 497
  role (desired) 499
  status 497
VRRP groups. See also VRRP.
vs RIP 237

W

warm start 55
warning message popup 72
warranty 756
  note 757
Web attack 428
Web Configurator 65
web configurator 54, 65
  access users 513
  admin users 65
web features
  ActiveX 479
  cookies 479
  Java 479
  web proxy servers 479
web proxy servers 261, 479
  see also HTTP redirect.
web-based SSL application 567
  configuration example 569
  create 568
webroot-directory-traversal attack 458
weighted round robin (for load balancing) 221
Windows Internet Naming Service. See WINS.
WinPopup window 709
WINS 183, 193, 202, 209, 326
  L2TP VPN 348
WINS server 193, 202, 209, 348
Wizard Setup 75
worm 403, 428
WWW 589
  and address groups 592
  and address objects 592
  and authentication methods 541, 592
  and certificates 590
  and zones 592
WWW. See also HTTP, HTTPS. 155, 589

Z

zones 113, 245
  and firewall 277, 285
  and FTP 605
  and interfaces 112, 245
  and SNMP 608
  and SSH 602
  and Telnet 604
  and VPN 245
  and WWW 592
  block intra-zone traffic 247, 279
  configuration overview 116
  extra-zone traffic 246
  inter-zone traffic 246
  intra-zone traffic 246
  prerequisites 117
  types of traffic with 245
  where used 117
ZyWALL
  configuration. See configuration.
  domain name 575
  system name 575
  terminology differences. See terminology differences.